KD

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 December 2002 (19.12.2002)

PCT

(10) International Publication Number
WO 02/102019 A2

(51) International Patent Classification[7]: H04L 29/06, 29/12, 12/14

(21) International Application Number: PCT/US02/12879

(22) International Filing Date: 22 April 2002 (22.04.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/285,419	20 April 2001 (20.04.2001)	US
60/301,532	26 June 2001 (26.06.2001)	US
09/956,376	18 September 2001 (18.09.2001)	US
10/082,422	22 February 2002 (22.02.2002)	US
10/082,487	22 February 2002 (22.02.2002)	US
10/082,489	22 February 2002 (22.02.2002)	US
10/082,423	22 February 2002 (22.02.2002)	US
10/086,009	27 February 2002 (27.02.2002)	US

(71) Applicant: 3COM CORPORATION [US/US]; 5400 Bayfront Plaza, Santa Clara, CA 95052 (US).

(72) Inventors: RUBINSTEIN, Alan; 585 Pickering Avenue, Fremont, CA 94536 (US). WANG, Gary; 10105 Crescent Road, Cupertino, CA 95014 (US). PATEL, Bhakt; 1080 McBain Avenue, Campbell, CA 95008 (US). CHANG, Yung-Fu; 5068 Forrest Glen Drive, San Jose, CA 95129 (US).

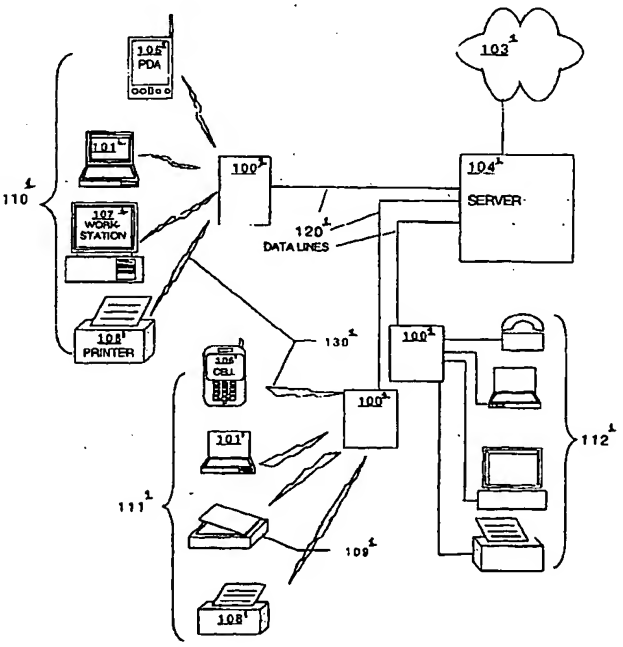
(74) Agents: GALLENSON, Mavis, S. et al.; LADAS & PARRY, 5670 Wilshire Boulevard, Suite 2100, Los Angeles, CA 90036 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR,

[Continued on next page]

(54) Title: NETWORK MANAGEMENT DEVICE AND METHOD



(57) Abstract: This disclosure reveals an apparatus for multiplexing signals in a network. The apparatus contains network connection devices and intelligent electronic circuitry for controlling and multiplexing data, voice telephone signals and power for multiple devices connected to the connection devices. The disclosure reveals a power management device for intelligent hardware; that is an intelligent data concentrator. Here a first interface is used to communicatively couple intelligent hardware to the network and a power source and a second interface for communicatively coupling the intelligent device to the plurality of client devices. The device processes and interprets data. The disclosure also reveals a secure network outlet for supporting IP device address assigning functionality and reducing the consumption of global device addresses within a network. The disclosure further reveals a flexible wireless communication network wherein first and second connection interfaces work with a device to concentrate data. The disclosure reveals an intelligent device that can be accessed remotely to reveal status information data. Finally, the disclosure reveals a method for managing access to a wireless personal area network in an intelligent concentrator. In this respect there is firewall protection, checking of an identification code for validity and access to the network and issuing an alert when a code is not valid.

WO 02/102019 A2

GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

NETWORK MANAGEMENT DEVICE AND METHOD

This disclosure is broken into six sections to facilitate the better understanding of this entire device. A short summary of each section is set forth before the section.

SECTION 1

The present invention relates to a method for managing access to a wireless personal area network in an intelligent concentrator. The method manages wireless access to a network by providing wireless communication in the network, providing firewall protection between the network and a wireless access device, receiving an identification code from the wireless access device to the network, determining whether the identification code is valid, granting network access to the wireless access device when the identification code is valid, denying network access to the wireless access device when the identification code is not valid, and issuing an alert to a network manager when the identification code is not valid. The identification code can be the unique media access code of the wireless access device or any other unique identification code previously registered with the network manager.

SECTION 1

This Section 1 relates to the field of Personal Area Networking (PAN) and access to those networks by various wireless access devices. More specifically, this Section 1 relates to a device and system for intelligently managing access to wireless networks.

BACKGROUND

Personal Area Networks are developing as adjuncts to local area networks (LANs). Modern personal area networking (PAN) generally refers to a small group of devices that communicate wirelessly and are normally within a small, personal, area. The PAN usually communicates with a network hub or a server that provides connection to a larger local area network (LAN) and to the Internet. Communication within the PAN is generally by RF or infrared devices and interface with the LAN is usually accomplished by cable connections between the wireless hub and the network server.

The wireless nature of a PAN implies the portability of the devices within it. Devices in the PAN are usually small and often battery powered such as laptop computers, personal data assistants (PDAs), or other wireless devices. There are also protocols for

implementing wireless network access for printers, scanners and other computer peripherals in the personal area network. With such portability, wireless access devices are easily transported between physical areas in the workplace as well as away from the workplace altogether.

Security and safety of data in a network can be jeopardized by uncontrolled access to a network by unauthorized users of wireless access devices, by authorized users in areas exposed to observation by unauthorized persons or computers, by users authorized in some areas but not in others, and by authorized network users with unauthorized devices. Wireless access removes what limited restrictions on access as are provided by wired connection.

Existing means of controlling access to wireless networks are similar to those used in the wired arena. They are typically centralized controls residing in a server in a network and dependent on the physical location of the connection point of the various access devices. Wireless access devices reduce the significance of physical location of connection points and thereby their utility in limiting access to authorized users.

What is needed, then, is means of controlling access to wireless networks, such as personal area networks, in order to provide security for those personal area networks against access by unauthorized users and unauthorized devices. Furthermore, such means should not be dependent on the permanent physical location of a connection point.

SUMMARY

Presented herein is a method for controlling access to wireless networks, such as personal area networks, in order to provide security for those personal area networks against access by unauthorized users and unauthorized devices. Furthermore, the method of providing such security is not dependent on the permanent physical location of a connection point.

The present invention relates to a method for managing access to a wireless personal area network in an intelligent concentrator. The method manages wireless access to a network by providing wireless communication in the network, providing firewall protection between the network and a wireless access device, receiving an identification code from the wireless access device to the network, determining whether the identification code is valid, granting network access to the wireless access device when the identification code is valid, denying network access to the wireless access device when the identification code is not valid, and issuing an alert to a network manager when the identification code is not valid. The identification code can be the unique media access code of the wireless access device or any other unique identification code previously registered with the network manager.

These and other objects and advantages of the present invention will become obvious to those of ordinary skill in the art after having read the following detailed description of the preferred embodiments which are illustrated in the various drawing figures.

BRIEF DESCRIPTION OF THE DRAWINGS

The operation of this invention can be best visualized by reference to the drawings.

Figure 1 illustrates a local area network with personal area network adjuncts and internet access.

Figure 2 illustrates a physical implementation of one embodiment of the present invention.

Figure 3 illustrates a physical implementation of one embodiment of the present invention.

Figure 4 illustrates a physical implementation of one embodiment of the present invention.

Figure 5 illustrates a block flow diagram of one embodiment of the present invention.

BEST MODE FOR CARRYING OUT THE INVENTION

Reference will now be made in detail to the preferred embodiments of the invention, examples of which are illustrated in the accompanying drawings. While the invention will be described in conjunction with the preferred embodiments, it will be understood that they are not intended to limit the invention to these embodiments. On the contrary, the invention is intended to cover alternatives, modifications and equivalents, which may be included within the spirit and scope of the invention as defined by the appended claims. Furthermore, in the following detailed description of the present invention, numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will be obvious to one of ordinary skill in the art that the present invention may be practiced without these specific details. In other instances, well-known methods, procedures, components, and circuits have not been described in detail so as not to unnecessarily obscure aspects of the present invention.

Some portions of the detailed descriptions that follow are presented in terms of procedures, logic blocks, processing, and other symbolic representations of operations on signals within an electronic circuit. These descriptions and representations are the

means used by those skilled in the electronic arts to most effectively convey the substance of their work to others skilled in the art. A procedure, logic block, process, etc., is here, and generally, conceived to be a self-consistent sequence of steps or instructions leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated in an electronic system.

Figure 1 illustrates a local area network that includes server 104 and distributed Intelligent concentrators 100 connected by data lines 120. Intelligent concentrators 100 act as wireless hubs for work centers 110 and 111 which results in each work center being implemented as a Personal Area Network (PAN). Note here that the term "personal area network" typically refers to a small network linked wirelessly to a larger local area network. Work center 112 is a hard-wired work center but acts in every way the same as a personal area networks except for the restricted motion of the hard-wired devices in the work center all connected to an intelligent concentrator 100. Note that the intelligent concentrator referred to in this discussion is one physical implementation of this

embodiment of the present invention. Other embodiments may be implemented in other physical devices.

Personal area network 110 is a typical PAN. It includes wireless access devices 105, a PDA enabled for wireless network access, laptop computer 101, work station 107, and network printer 108. Each of these wireless access devices communicates with intelligent concentrator 100 by means of wireless communication 130 which may be a radio frequency (RF) protocol, such as Bluetooth or some other RF protocol, or infrared (IR).

Note that wireless communication enables and implies a temporary nature to the specific suite of wireless access devices within the personal area network. A user may carry a PDA at all times while moving about the workplace, or even when outside of the workplace, and access the network with it only occasionally. Data-enabled cell phone 106, shown communicating with intelligent concentrator 135 in personal area network 111, is another highly portable wireless access device that would likely access the wireless network on an occasional basis. Yet another possible wireless access device is illustrated by scanner 109. In this embodiment of the present invention, the intelligent concentrators, 100, are enabled to determine, by this embodiment of the present

invention and upon each attempt to access the network, whether each wireless access device is an authorized device.

An intelligent concentrator, illustrated at 100 in Figure 1, is easy to install and reliably provides a hub and connection point for access to Voice & Data Networks. The embodiment of the present invention discussed here is implemented through miniaturized hardware that could be installed inside a wall or in an internal space provided for in an office cubicle. Power is easily supplied using the same hardware, either locally or remotely over network cabling. Access to device power is simultaneously accessible with data line connection in a wired connection. Wireless access devices are commonly battery powered or receive power from some other source.

Figure 2 illustrates a possible configuration for the physical implementation of an embodiment of the present invention. Intelligent concentrator 200 is shown in side cutaway view, with connector jacks 204 for possible wired connections and wireless communication device 207 shown in one of several conceivable arrangements. Wireless communication device 207 is envisioned as being enabled in a variety of protocols. Multiplexing of signals to and from server 104 would very likely be under the control of in-unit electronics suite 202. Those signals, in one embodiment of the

present invention, would be multiplexed onto single cable 100 and connect to intelligent concentrator 200 via back-of-unit connector 206.

Also shown in Figure 2 is an add-on device 203. A range of possibilities exists for the functions of device 203. It could be implemented as an intelligent device, capable of being remotely tested, allowing the network infrastructure and integrity of the network cabling to be tested and evaluated from a central location, without any action being required at the work site. Device 203 can also be implemented as a physical security device, capable of preventing physical attachment to the LAN cabling without a notification being sent to the server that the physical network port has been compromised. Device 203 can also simply be a dust cover installed on an intelligent concentrator that is only involved in a wireless personal area network, obviating the need for wired connectors 204. In one embodiment, wired connectors 204 are implemented as standard communications jacks, such as RJ45. Additionally, status indicator lights are mounted on the surface of the intelligent concentrator in another embodiment.

Figure 3 illustrates one configuration for the user-accessible face of an intelligent concentrator, one physical implementation of

this embodiment of the present invention. Intelligent concentrator 100' is shown here with four RJ-45 jacks, 204'. There is space, even if an intelligent concentrator takes the form factor of a standard wall plate device, for more jacks, 308'. These other jacks could enable a parallel connection to a different network or to a telephone system independent of a LAN or to a number of other envisioned possibilities. Figure 3' also shows status indicator light 305' which could be implemented in another implementation of this embodiment.

Again shown, in Figure 3', is wireless communication device 207'. Device 207' can be implemented in any number of wireless standards for wireless connection to the network. The necessary transceiver electronics for device 207' are contained in the body of concentrator 100', integral with internal electronics 202' in Figure 2'. Other implementations could implement the circuitry in other ways, however. Power for communications device 207' and its associated circuitry can, like that for intelligent electronic circuitry 202' and device 203', be received via multiplexed cabling.

Figure 4' illustrates one implementation for supplying device power. Here utility socket 320' is shown in order to illustrate the application of high voltage or current power that reaches the intelligent concentrator via cabling parallel to the data cabling.

With access to the power being through intelligent concentrator 200, management and control of a power supply to a device can still be maintained even though the data is communicated wirelessly. The illustration of a utility power socket is not meant to imply that there is some special application of utility AC power in this embodiment. It is solely meant to illustrate a parallel application of high-voltage power through an intelligent concentrator.

Figure 5 illustrates a block flow diagram of one embodiment of the present invention. There, in process 500, a distributed firewall is provided at 510 for each applicable network work center. Network wireless access devices, such as computers, PDAs, data-enabled cell phones, and computer peripherals, attempt network access by submitting a unique identification code which is received by the distributed firewall at 520. At 530, the submitted identification code is compared to a list of valid, registered identification codes. If the submitted code is valid, 540, network access is granted at 570 and the process ends at 599. If the identification code is not valid, network access is denied at 550 and an alert flag is raised to the network manager, 560. Again, the process ends at 599.

A significant advantage offered by this embodiment is in the uniqueness of the list of valid identification codes, in this

embodiment media access codes (MACs), that is supplied to each distributed firewall when the network is started. Note that the MAC (Media Access Control) address is a device's unique hardware number. On an Ethernet LAN, it is generally the same as the device's ethernet address. When a device is connected to the Internet from a computer or host, a correspondence table relates the IP address to the computer's physical address on the LAN.

Each distributed firewall has its own unique identification with the network manager and is given the list of codes applicable to that particular distributed firewall. The network manager, for example, can have a wireless laptop computer whose identification code is on every list issued in the network. Then the network manager can access the network from any personal area network location in the entire network. A personal area network user can have a PDA that is valid for access at the user's workstation and also at a laboratory that the user often works in.

In another example of the utility of this embodiment of the present invention, if two users have personal area networks adjacent to each other, their wireless access devices have unique codes that are not found on each other's applicable valid code list. In that way, restrictions can be implemented that prevent cross-

talk between personal area networks and can also provide a layer of network authorization management.

Some distributed firewalls can be implemented with unlimited valid codes but with limited network access to wireless devices that access the network though those firewalls. This is useful in a company lobby where visitors can use their own wireless access devices to access the network as far as phone directories and promotional information but not as far as entry into restricted network areas.

In one embodiment of the present invention, the distributed firewall is implemented as firmware in an intelligent concentrator. In another embodiment, the firewall is implemented as software in a wireless network hub where it is in control of access from several personal area networks that are centered on the same physical hub. A common thread between these implementations is the distributed access control afforded to the distributed firewalls by the separate maintenance of the valid access code lists.

Each list in this embodiment of the present invention contains information such as a unique firewall identification code, the physical residency and location of the firewall, a list of designated users, and a list of registered MAC addresses. The list of users for a

work station personal area network can be as small as to include only the network manager and the personal area networks primary user. The list for a firewall associated with a conference room, for example, can have no restrictions on users but significant limitations on network resources that are accessible from the conference room.

The number of possible variations in access lists is limited only by network and workplace needs. This embodiment affords an extremely adaptable wireless network access management tool to the network manager.

The foregoing descriptions of specific embodiments of the present invention have been presented for purposes of illustration and description. They are not intended to be exhaustive or to limit the invention to the precise forms disclosed, and obviously many modifications and variations are possible in light of the above teaching. The embodiments were chosen and described in order to best explain the principles of the invention and its practical application, to thereby enable others skilled in the art to best utilize the invention and various embodiments with various modifications as are suited to the particular use contemplated. It is intended that the scope of the invention be defined by the Claims appended hereto and their equivalents.

SECTION 2

A method for efficiently managing a network using intelligent hardware. An intelligent device is provided, wherein the intelligent device is communicatively coupled to a voice or data network. The intelligent device is configured to communicatively couple a plurality of electronic devices to the network. Status information data of the intelligent device is accessed such that the intelligent device is configured to be monitored remotely. In one embodiment, the intelligent device comprises a first interface for communicatively coupling the intelligent device to the network and a second interface for communicatively coupling the intelligent device to the plurality of client devices. The intelligent device also comprises means for processing and interpreting data coupled to the first interface, and status information provision means coupled to the means for processing and interpreting data. In one embodiment, the status information provision means is configured to obtain the status information data of the intelligent device and is configured to provide status information data for remote access.

SECTION 2

This Section 2 relates to the field of computer networks. In particular, this Section 2 relates to a method for efficiently managing a network using intelligent hardware.

BACKGROUND

Present computer networks often are comprised of hundreds or thousands of computer systems and other electronic devices (e.g., printers, personal digital assistants, and VOIP-enabled voice telephones). These computer systems and electronic devices each consume varying amounts of network resources at various times. As a result, it can be extremely challenging for Information Services (IS) personnel to efficiently manage large networks.

One challenge facing IS personnel is that it is often difficult to know the status (e.g., data transfer information) of a particular computer system or electronic device on the network at a particular time. This information is desirable as it can assist the IS personnel in efficiently managing the resources of the network by helping them to understand the present needs of the network. Furthermore, the status information can be used to aid in fault detection on the network.

Since IS personnel are often responsible for a very large number of computer systems and electronic devices coupled to the network, it is desirable to be able to monitor the activity of the network from a central location. While current networks often have a central location for monitoring the network, it is difficult to monitor the activity of each computer system or electronic device. Typically, computer systems are coupled to routers or hubs. While it is possible to monitor the activity into the hubs and routers, it is not possible to monitor the activity out because the hubs do not possess the intelligence necessary to provide such information.

Another concern of IS personnel is to ensure that the network is secure. It is essential for IS personnel to be aware of all network activity, so that they are aware of suspicious use of the network. For example, if a certain computer system is accessing the network at a time when it should not be, the IS personnel need to be aware of this so they can investigate. Furthermore, in the event that it is determined that inappropriate activity is occurring at a computer system, it is desirable that the IS personnel be able to shut down the computer system. Furthermore, physical asset security is another problem facing IS personnel today.

IS personnel need to manage the resources that are connected by local area networks (LANs) which often are comprised of multiple routers, switches and hubs. The networks that exist tend to grow and evolve over time; the

physical locations of a specific PC often will shift over time. These changes can occur when an employee moves to join a new group or is relocated from location another within the office. Typically, the specific location of a computer system in the workplace is not easily recalled as records are often not kept or age rapidly and become out of date. Even in situations where a record exists, the patch cable connecting a computer system to a switch port is often changed in the wiring closet without any formal recording of the change.

An IS person may know that a specific PC is the source of network problem or needs to be visited by a technician to provide service. IS can identify a machine by examining an identifier such as the hard coded MAC address of it's Network Interface Card (NIC), but while this information is necessary it is not sufficient to provide any real guidance as to the physical location of the PC. The IS person may also know that a problem exists with a machine that is bound to an IP address (either static or dynamically assigned). However, while necessary the knowledge of the IP address by itself is not sufficient to locate the computer.

Furthermore, current network management techniques are not easy to use, and require a significant amount of training. It is desirable that network management systems be easy to use as well as inexpensive.

Accordingly, a need exists for a method and device thereof for efficiently managing a network. Also, a need exists for a method and a device thereof that accomplishes the above need and is controlled from a remote management station. Also, a need exists for a method and a device thereof that accomplishes the above needs and aids in managing the security of a network. Finally, a needs exists for a method and a device thereof that accomplishes the above needs and is easy to use.

SUMMARY OF THE INVENTION

The present invention provides a method and device thereof for efficiently managing a network. The present invention also provides a method and a device thereof that is controlled from a remote management station. The present invention also provides a method and a device thereof for aiding in managing the security of a network. Finally, the present invention also provides a method and a device thereof that accomplishes the above and is easy to use.

A method for efficiently managing a network using an intelligent device is provided. An intelligent device is provided, wherein the intelligent device is communicatively coupled to a voice or data network. The intelligent device is configured to communicatively couple a plurality of electronic devices to the network. Status information data of the intelligent device is accessed such that the intelligent device is configured to be monitored remotely.

In one embodiment, the intelligent device comprises a first interface for communicatively coupling the intelligent device to the network and a second interface for communicatively coupling the intelligent device to the plurality of client devices. The intelligent device also comprises means for processing and interpreting data coupled to the first interface, and status information provision means coupled to the means for processing and interpreting data. In one embodiment, the status information provision means is configured to

obtain the status information data of the intelligent device and is configured to provide status information data for remote access.

In one embodiment, the intelligent device is communicatively coupled over the network to a computer system for accessing the status information provision means. In one embodiment, the computer system is a remote monitoring unit.

In one embodiment, the computer system comprises a display for displaying the status information of the intelligent device. In one embodiment, the display comprises a graphical user interface configured for allowing a user to interact with the status information of the intelligent device. In one embodiment, the display is for displaying a graphical representation of the network.

In one embodiment, the intelligent device is coupled to a power source over the network, the power source for providing power to the intelligent device. In one embodiment a power level of the intelligent device is controlled over the network.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and form a part of this specification, illustrate embodiments of the invention and, together with the description, serve to explain the principles of the invention:

FIGURE 1 illustrates an exemplary wired desktop cluster coupled to a local area network (LAN) in accordance with one embodiment of the present invention.

FIGURE 2 is a block diagram of a cross-sectional view of an intelligent data concentrator in accordance with one embodiment of the present invention.

FIGURE 3 is an illustration of a perspective view of an exemplary faceplate of an intelligent data concentrator in accordance with one embodiment of the present invention.

FIGURE 4 is a block diagram of an exemplary LAN upon which embodiments of the present invention may be practiced.

FIGURE 5 is a flowchart diagram of the steps in a process for efficient management of a network using an intelligent device (e.g., an intelligent data

concentrator) for providing access to voice and data networks in accordance with one embodiment of the present invention.

FIGURE 6 is a block diagram of an intelligent data concentrator configured for performing a process of efficient management of a network in accordance with an embodiment of the present invention.

FIGURE 7 is an exemplary screen shot of a display for displaying a network comprising a plurality of intelligent devices in accordance with an embodiment of the present invention.

FIGURE 8 illustrates an exemplary computer system platform upon which embodiments of the present invention may be practiced.

DETAILED DESCRIPTION

In the following detailed description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that the present invention may be practiced without these specific details. In other instances, well-known structures and devices are not described in detail in order to avoid obscuring aspects of the present invention.

Some portions of the detailed descriptions which follow are presented in terms of procedures, steps, logic blocks, processing, and other symbolic representations of operations on data bits within a computer memory. These descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. A procedure, computer executed step, logic block, process, etc., is here and generally conceived to be a self-consistent sequence of steps of instructions leading to a desired result. The steps are those requiring physical manipulations of data representing physical quantities to achieve tangible and useful results. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers or the like.

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely

convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussions, it is appreciated that throughout the present invention, discussions utilizing terms such as "providing", "accessing", "coupling", "monitoring", "managing" or the like, refer to the actions and processes of a computer system, or similar electronic computing device, such as intelligent hardware or an intelligent data concentrator. The computer system or similar electronic device manipulates and transforms data represented as electronic quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission, or display devices.

Portions of the present invention are comprised of computer-readable and computer executable instructions which reside, for example, in computer-usable media of a computer system or intelligent hardware (e.g., an intelligent data concentrator). It is appreciated that the present invention can operate within a number of different computer systems including general purpose computer systems, embedded computer systems, and stand alone computer systems specially adapted for controlling automatic test equipment.

The present invention provides a method for efficiently managing a network using intelligent hardware, also referred to herein as an intelligent data concentrator. The described method can be controlled from a computer system communicatively coupled to the intelligent device over the network. In one embodiment, the computer system is a remote monitoring unit.

Figure 1 illustrates an exemplary personal area network (PAN) 100 coupled to a local area network (LAN) 150 in accordance with one embodiment of the present invention. PAN 100 comprises IP telephony 110, notebook 120, desktop workstation 130, and printer 140, each of which is communicatively coupled to intelligent data concentrator 210. Intelligent data concentrator 210 is coupled to LAN 150, thus acting as an interface from the various client devices (e.g., comprises IP telephony 110, notebook 120, desktop workstation 130, and printer 140) to LAN 150.

In one embodiment, the electronic devices of PAN 100 (e.g., comprises IP telephony 110, notebook 120, desktop workstation 130, and printer 140) receive power over LAN 150 through intelligent data concentrator 210. In the present embodiment, a remote power source transmits power across LAN 150 to intelligent data concentrator 210. In one embodiment, electronic devices coupled to intelligent data concentrator 210 are configured to receive the power they require to operate over LAN 150.

Figure 2 is a block diagram 200 of a cross-sectional view of an intelligent data concentrator 210 in accordance with one embodiment of the present invention. This embodiment of the present invention implements intelligent hardware that is easy to install and reliably provides an attachment point for access to voice and data networks 240. The embodiment is implemented through miniaturized hardware that can be installed inside of a wall or in internal space provided for in an office cubicle. One surface 230 of this embodiment is intended to be accessible by the end user and would in most instances be on an external surface of a workspace.

A plurality of ports 220 are mounted on the external surface 230 of this embodiment. In one embodiment, communication port 220 is an RJ-45 jack. In another embodiment, port 220 is an RJ-11 jack. It should be appreciated that port 220 is not limited to any particular jack, and that any type of communication port can be used. Additionally, while intelligent data concentrator 210 illustrates four ports 220, it should be appreciated that alternative implementations could support a greater or lesser number of ports 220.

Connections to the central data (LAN) or voice network 240 are terminated at intelligent data concentrator 210 for coupling to ports 220. Termination of the network cabling 250 (voice or data) will provide for both a

reliable electrical and mechanical connection for industry standard communications cabling such as CAT-3, CAT-5, CAT-5E or similar cabling.

In one embodiment, intelligent data concentrator 210 receives power over network cabling 250 from network 240. A remote power source 260 transmits power over network cabling 250 to provide intelligent data concentrator 210 with the power it requires to operate. In one embodiment, intelligent data concentrator 210 is configured to transmit power to connected electronic devices through ports 220.

Figure 3 is an illustration of a perspective view 300 of an exemplary user-accessible surface 230 of an intelligent data concentrator 210 in accordance with one embodiment of the present invention. A user is able to connect data devices to a voice or data network through ports 220. As described above, in one embodiment of the present invention, intelligent data concentrator 210 is configured to transmit power to connected electronic devices through ports 220.

Figure 4 is a block diagram of an exemplary LAN 400 upon which embodiments of the present invention may be practiced. In one embodiment, LAN 400 comprises a remote monitoring unit 405 and intelligent hardware 410, 415, and 420. In one embodiment, remote monitoring unit 405 is a computer system (e.g., computer system 100 of Figure 1). However, it should be

appreciated that remote monitoring unit 405 may be another electronic device configured for managing networks (e.g., a router or a hub).

In one embodiment, intelligent hardware 410, 415 and 420 are intelligent data concentrators (e.g., intelligent data concentrator 210 of Figure 2 or intelligent data concentrator 602 of Figure 6). In one embodiment, remote monitoring unit 405 can access the intelligence (e.g., intelligence 612 of Figure 6) of intelligent hardware 410, 415 and 420. In another embodiment, remote monitoring unit 405 is a central data switch or hub. Intelligent hardware 410, 415 and 420 are communicatively coupled to remote monitoring unit 405 over links 440, 445 and 450, respectively. In one embodiment, links 440, 445 and 450 are network cabling. In one embodiment, links 440, 445 and 450 also are coupled a power source (e.g. power source 250 of Figure 2 or power source 609 of Figure 6), such that they provide power to intelligent hardware 410, 415 and 420.

In one embodiment, intelligent hardware 410, 415 and 420 are connected to remote monitoring unit 405 by means of network cabling. In the current embodiment, CAT 3 or 5 cabling is used and an Ethernet physical interface is employed. However, it should be appreciated that the present invention will work with other types of LANs, such as LANs with differing physical connections or adopted for use in RF wireless and optical systems. As discussed above, in one embodiment, links 440, 445 and 450 also provide

power to intelligent hardware 410, 415 and 420. In one embodiment, the power is supplied over network cabling.

Intelligent hardware 410 is coupled to electronic devices 425a and 425b. Similarly, intelligent hardware 415 is coupled to electronic devices 430a, 430b and 430c, and intelligent hardware 420 is coupled to electronic devices 435a and 435b. It should be appreciated that electronic devices can comprise any number of data devices or client devices, including but not limited to: computer systems, printers, voice IP telephones, and fax machines configured for use over voice IP networks.

In one embodiment, the intelligent hardware is configured to provide power to connected electronic devices. For example, in the present embodiment, intelligent hardware 410 supplies power to electronic devices 425a and 425b. It should be appreciated that electronic devices connected to an intelligent hardware may receive power over LAN 400. Power is supplied to the intelligent hardware, and an electronic device configured to receive power through the intelligent hardware receives its operating power through the intelligent hardware.

Figure 5 is a flowchart diagram of the steps in a process 500 for efficient management of intelligent hardware (e.g., an intelligent data concentrator) for providing access to voice and data networks. Steps of process 500, in the

present embodiment, may be implemented with any computer languages used by those of ordinary skill in the art.

At step 510, an intelligent device (e.g., intelligent data concentrator 210 of Figure 2 or intelligent data concentrator 602 of Figure 6) is provided, wherein the intelligent device is communicatively coupled to a voice or data network. The intelligent device is for communicatively coupling electronic devices to a network. The intelligent device comprises a status information provision means and is configured such that the intelligent device is configured to be monitored remotely. The status information provision means is configured to obtain status information of the intelligent device and provide the status information for remote access.

At step 520 of process 500, the status information provision means of the intelligent device is accessed over the network. The status information data of the intelligent device is accessed such that the intelligent device is configured to be monitored remotely.

In one embodiment, the intelligent device is communicatively coupled over the network to a computer system for accessing the status information provision means. In one embodiment, the computer system is a remote monitoring unit. . In one embodiment, the described method can be controlled from a remote monitoring unit by an information technology (IT) manager. In

another embodiment, the present invention may be controlled from any computer system on the network, subject to security safeguards.

In one embodiment, the computer system or remote monitoring unit comprises a display (e.g., display device 805 of Figure 8) for displaying the status information of the intelligent device. In one embodiment, the display comprises a graphical user interface configured for allowing a user to interact with the status information of the intelligent device. In one embodiment, the display is for displaying a graphical representation of the network.

In one embodiment, over the network, the IT manager at the remote monitoring unit is able to monitor the activity of each intelligent concentrator. The IT manager is able to graphically view the current activity of an intelligent concentrator. In one embodiment, a computer system with a graphical user interface is used, wherein the network is displayed on a computer screen (e.g., screen shot 700 of Figure 7). Each intelligent concentrator is depicted as a screen icon. By interacting with the icon for a particular intelligent concentrator, it is determined what activity the intelligent concentrator is currently performing.

In another embodiment, the present invention creates a physical view drawing of the network. In the present embodiment, the drawing of the network is displayed on the computer screen of a computer system with a graphical user interface.

In one embodiment, the intelligent device is coupled to a power source over the network, the power source for providing power to the intelligent device. In one embodiment, a power level of the intelligent device is controlled over the network. In one embodiment, the power level is controlled at a computer system connected to the network. In another embodiment, an IT manager can control the power of an intelligent concentrator, such that the IT manager may turn the device on or off. This is an effective tool for managing the use of intelligent concentrators in both IT management and security scenarios.

In another embodiment, a log is created for each intelligent concentrator is created and stored. By interacting with an icon for a particular intelligent concentrator, it is determined what activity the intelligent concentrator has performed over the length of the log. In one embodiment, the log is stored at a remote computer system or remote monitoring unit. In another embodiment, the log is stored in the intelligent device.

In one embodiment, the intelligent device is configured to be assigned a distinct device location identifier associated therewith. In one embodiment, the device location identifier is pre-configured into the intelligent device. In another embodiment, the device location identifier is assigned at installation. By assigning each intelligent concentrator a distinct device location identifier, the

network can be mapped and managed with greater ease, as the location and connections for each intelligent device can be monitored.

In one embodiment, the intelligent device allows for the recording of the physical location of a connected electronic device and actively monitor the MAC address or the IP addresses of the networked devices that are attached to it. In another embodiment, the intelligent device is installed in close proximity to the attached devices such that knowledge of the location of the intelligent device is equivalent to knowing the physical location of the attached asset (e.g., a computer system or networked printer).

In one embodiment, device location identifier is stored in a non-volatile storage element. The present embodiment allows the device location identifier to remain intact in the face of power outages or intentional powering down to the intelligent device during servicing or as part of a system power management scheme. In one embodiment, the

In one embodiment, the device location identifier is subject to inadvertent or intentional modification by unauthorized users since corruption of the stored location information can hinder the maintenance of the network assets and can reduce network security provided to the attached assets.

In one embodiment, the specific identification string that is used to call

out a device location identifier is flexible. In one embodiment, traditional numeric identifiers such as cubicle or workspace numbers can be used. In another embodiment, the naming conventions used to identify a workspace or conference room are used.

In one embodiment, the device location identifier is entered by a client device communicatively coupled with the intelligent device. In one embodiment, the client device is wirelessly coupled to the intelligent device. In another embodiment, the client device is coupled to the intelligent device over a wired connection. In one embodiment, the device location identifier is entered into the intelligent device by a programming port provided for this purpose. In another embodiment, the device location identifier is entered into the intelligent device over the network.

In one embodiment, the device location identifier is intended to permanently bind the intelligent device to a specific location so as to prevent unauthorized access to or modification of this data. In one embodiment, lockout mechanisms exist to prevent local or remote modification or corruption of this information. In one embodiment, the lockout mechanism authenticates a station through Challenge Access Protocol (CHAP) where a hard coded serial number entered into the unit at manufacture serves as the user name in a handshake with a management/configuration station that is used to enter the device location.

In one embodiment, an inventory of the MAC addresses that are connected to specific intelligent devices can be made over the network connections. If an asset (e.g., a computer system, a printer or another networked device) is moved or removed this event can be detected. If remote network based power on mechanisms exist in the NICs of the attached computer systems or other network attached devices, a spot inventory can be taken without regard to the current power status of the computer system that is connected to the intelligent device. In another embodiment, having the intelligent device examine the NIC's MAC address can restrict access control to a network point of presence in a specific area.

Figure 6 is a block diagram 600 of an intelligent data concentrator 602 configured for performing a process of efficiently managing a network using intelligent hardware in accordance with an embodiment of the present invention.

Intelligent data concentrator 602 comprises a first interface 604 for communicatively coupling intelligent data concentrator 602 to network 608 and for receiving power transmitted from power source 609 over network 608. Intelligent data concentrator 602 also comprises a plurality of second interfaces 606a-d for communicatively coupling intelligent data concentrator 602 to a plurality of electronic devices 610a-d. In one embodiment, second

interfaces 606a-d are communication ports (e.g., communication ports 220 of Figure 2). It should be appreciated that there can be any number of second interfaces 606a-d, and that the present invention is not meant to limit the number of second interfaces 606a-d. First interface 604 operating in conjunction with second interfaces 606a-d operates to connect electronic devices 610a-d to network 608.

In another embodiment, second interfaces 606a-d are configured to provide power to connected electronic devices. In the present embodiment, first interface 604 operating in conjunction with second interfaces 606a-d operates to connect electronic devices 610a-d to power source 609, thus providing electronic devices 610a-d with power.

Intelligent data concentrator 602 also comprises intelligence 612. In one embodiment, intelligence 612 comprises means for processing and interpreting data 614 coupled to the first interface 604 and status information provision means 616 coupled to the means for processing and interpreting data 614. Means for processing and interpreting data 614 is intended to include, but not limited to: a processor, a robust processor and a central processing unit (CPU).

In one embodiment, status information provision means 616 is a software implementation (e.g., a hardware power mode controller) in intelligent

data concentrator 602². Alternatively, status information provision means 616² can be implemented by hardware or firmware (e.g., a software or firmware power mode controller).

In one embodiment, status information provision means 616² operates to obtain status information of intelligent data concentrator 602² (e.g., data transfer between first interface 604² and second interfaces 606a-d)², and to provide access to the status information.

In one embodiment, status information provision means 616² operates in conjunction with a remote monitoring unit (e.g., remote monitoring unit 405² of Figure 4)² of network 608² for performing efficient management of network 608². In another embodiment, status information provision means is controlled by a remote monitoring unit (e.g., remote monitoring unit 405² of Figure 4)² for accessing the status information of intelligent data concentrator 602².

Figure 7² is an exemplary screen shot 700² of a display (e.g., display device 805² of Figure 8)² for displaying a network comprising a plurality of intelligent devices in accordance with an embodiment of the present invention. In one embodiment, the present invention creates a graphical representation (e.g., a physical view drawing) of network 720². In the present embodiment, the drawing of network 720² is displayed on the computer screen (e.g., display device 805² of Figure 8)² of a computer system with a graphical user interface.

In one embodiment, the drawing of network 720² comprises screen icons 730², 740² and 750². In one embodiment, icon 730² represents a remote monitoring unit or a central computer system. In one embodiment, icon 740² represents an intelligent device (e.g., intelligent data concentrator 210² of Figure 2²). In one embodiment, icon 750² represents an electronic device coupled to an intelligent data concentrator. It should be appreciated that there can be any number of devices (e.g., computer systems, hubs, routers, switches, intelligent data concentrators and coupled electronic devices) shown on screen 710².

In one embodiment, over the network, the IT manager at the remote monitoring unit is able to access the activity of each intelligent concentrator. The IT manager is able to graphically view the current activity of an intelligent concentrator. By interacting (e.g., operating cursor control device 807² of Figure 8²) with the icon for a particular intelligent concentrator, it is determined what activity the intelligent concentrator is currently performing.

Refer now to Figure 8² which illustrates an exemplary computer system 800² upon which embodiments of the present invention may be practiced. In general, computer system 800² comprises bus 810² for communicating information, processor 801 coupled with bus 810² for processing information and instructions, random access (volatile) memory (RAM) 802² coupled with bus 810² for storing information and instructions for processor 801², read-only

(non-volatile) memory (ROM) 803[2] coupled with bus 810[2] for storing static information and instructions for processor 801[2], data storage device 804[2] such as a magnetic or optical disk and disk drive coupled with bus 810[2] for storing information and instructions.

In one embodiment, computer system 800[2] comprises an optional user output device such as display device 805[2] coupled to bus 810[2] for displaying information to the computer user, an optional user input device such as alphanumeric input device 806[2] including alphanumeric and function keys coupled to bus 810[2] for communicating information and command selections to processor 801[2], and an optional user input device such as cursor control device 807[2] coupled to bus 810[2] for communicating user input information and command selections to processor 801[2]. Furthermore, an optional input/output (I/O) device 808[2] is used to couple computer system 800 onto, for example, a network.

Display device 805[2] utilized with computer system 800[2] may be a liquid crystal device, cathode ray tube, or other display device suitable for creating graphic images and alphanumeric characters recognizable to the user. Cursor control device 807[2] allows the computer user to dynamically signal the two-dimensional movement of a visible symbol (pointer) on a display screen of display device 805[2]. Many implementations of the cursor control device are known in the art including a trackball, mouse, joystick or special keys on

alphanumeric input device 806 capable of signaling movement of a given direction or manner of displacement. It is to be appreciated that the cursor control 807 also may be directed and/or activated via input from the keyboard using special keys and key sequence commands. Alternatively, the cursor may be directed and/or activated via input from a number of specially adapted cursor directing devices.

The preferred embodiment of the present invention, a method for efficiently managing a network using intelligent hardware, is thus described. While the present invention has been described in particular embodiments, it should be appreciated that the present invention should not be construed as limited by such embodiments, but rather construed according to the below claims.

SECTION 3

The present invention is a flexible wireless communication network connection point that provides convenient and effective connection of network devices to a network. In one embodiment the present invention is a multi-configuration network connection point device comprising a first connection interface, a second connection interface, a means for intelligently concentrating data and a communication bus. The first connection interface includes a primary connection port for communicatively coupling to an upstream network device. The second connection interface including a secondary connection port for communicatively coupling to a downstream network device via a wireless technology. In one exemplary implementation the second connection interface is adapted to be secured in a fixed location while conveniently providing the communicative coupling to a downstream network device via a wireless technology. The means for intelligently concentrating data concentrates data from a plurality of interface connection ports included in the second connection interface for communication on the primary connection port of the first connection interface. The communication bus communicatively couples the first connection interface to the second connection interface.

BACKGROUND

Section 3

This Section 3 relates to the field of communication networks. In particular, this Section 3 relates to a system and method for providing concentrated access to a communication network by wireless devices.

Related Art

Electronic systems and circuits have made a significant contribution towards the advancement of modern society and are utilized in a number of applications to achieve advantageous results. Numerous electronic technologies such as digital computers, calculators, audio devices, video equipment, and telephone systems facilitate increased productivity in analyzing and communicating data, ideas and trends in most areas of business, science, education and entertainment. Often these advantageous results are realized and maximized through the use of distributed resources. Utilizing distributed resources usually involves numerous devices relying on

various communication mediums to communicate with each other. However, providing convenient communication network connections capable of accommodating a variety of communication devices is often expensive and very difficult.

Communication technologies are advancing at an incredible rate in significantly different directions due to the advantages provided by different configurations and implementations. Networks can be arranged in numerous configurations comprising a variety of network types. Some of the most popular types of networks comprise Ethernet (coaxial cable or twisted-pair cable), token ring, Fiber Distributed Data Interface (FDDI), Frame Relay, Integrated Services Digital Network (ISDN), X.25, and Synchronous Data Link Control (SDLC). Different communication protocols usually have different advantages. The different advantageous characteristics of communication protocols or configurations often tend to be somewhat mutually exclusive and the utilization of a particular communication architecture usually results in a trade off of benefits. Hardwire communication networks and wireless communication networks are one example of two protocols that tend to have mutually exclusive characteristics such as inversely proportional bandwidth and portability attributes.

Hardwired networks typically provide significant bandwidth and are better equipped to satisfy significant communication requirements associated

with advanced and complicated end use applications. However, hardwire communication networks involve the installation of significant infrastructure resources that are relatively expensive to install and maintain. For example, traditional communication networks such as a local area network (LAN) typically have multiple parallel cable or communication bus runs to end use devices at each worksite. The parallel runs are a significant portion of the resources an d costs associated with installation of a network, the more parallel runs the greater expenditure or resources. Hardwired devices also typically require a connection to a central power supply (such as utility power) and the power is usually delivered by separate cable runs. The portability of the end use devices in a hardwired system is usually hindered and limited by the "tethered" connection to a network.

Wireless communications technologies tend to offer a number of benefits not readily available in hardwired systems. For example, wireless communication devices usually provided ease of use and greater mobility. However, wireless devices tend to have characteristics that are limited with regard to certain desirable features. For example, wireless communication devices tend have relatively limited bandwidth compared to hardwired communication systems. The operation of wireless devices also tends to be limited by the amount of the power available (e.g., batteries) in the portable device. The reliability of wireless communications are also generally susceptible to adverse impacts due to affects such as loss or deterioration of

signal due to noise, interference, distance, etc., and are more susceptible to security infiltration and illicit activities.

Many of the adverse affects encountered in a communications network are related to the manner in which devices are "connected to" the communication network. Typically, communications protocols between major communication network facilities (such as a plurality of head end host devices or central switching centers) have characteristics that lend themselves to fixed unchanging connection mechanisms that are resource extensive and undesirable (e.g., overkill) for most downstream end use connections. However, it is usually desirable for downstream connections to be flexibly capable of accommodating a wide variety of differently configured end use devices. Downstream end use connections to a communication network are often initially made at a local area network (LAN) with different downstream end use devices (such as a group of personal computers (PC), printers, faxes, etc.) located in a home or single business site (location). Traditional attempts at accommodating initial connections to a communications network are usually ad hoc, of questionable reliability, resource intensive (such as separate communication paths and connections to upstream facilities for each connection), inefficiently managed and subject to failures (e.g., caused by accidental breakage or removal of a wire).

There are a number of other desirable communication network features that are often critically impacted by a communication network connection point. For example, maintenance troubleshooting and fault detection are usually complicated and resource intensive activities. Traditional technologies sometimes rely upon separate stand alone connection points (such as connection points in unanchored boxes) that are susceptible to movement, attempted tampering or accidental damage (such as coffee spills, getting knocked over, hit, jarred, etc.) by ordinary end users that do not have the requisite knowledge or skill to participate in network facility administration activities. Some traditional attempts at correcting communication problems are directed to connections dedicated on a per user or end use device basis and these very "rigid" approaches tend to remove a desirable level of end user connection flexibility. While the flexibility of users being able to easily move end use devices to different locations or connect different devices to a connection point is advantageous and convenient, the potential movement of the stand alone connection points by end users rather than network maintenance personnel is not desirable since it tends to introduce additional variables to a troubleshooting process.

Traditional end use connection points are also often vulnerable to security breaches. Some traditional security approaches rely upon software security solutions but these usually require constant maintenance and management and are subject to attacks through common hacking techniques.

For example, stand alone connection points are susceptible to illicit interaction behind a firewall. An additional weakness of traditional software solutions is that the end use device to be networked may not be able to host requisite software. Wireless communications are particularly vulnerable to illicit interception. Wireless communications are usually broadcast over long distances covering publicly accessible spaces making interception relatively easy.

Accordingly, what is required is a flexible communications network connection point that provides convenient and effective connection of network devices to a network.

SUMMARY

The present invention is a flexible wireless communication network connection point that provides convenient and effective connection of network devices to a network. In one embodiment the present invention is a multi-configuration network connection point device comprising a first connection interface, a second connection interface, a means for intelligently concentrating data and a communication bus. The first connection interface includes a primary connection port for communicatively coupling to an upstream network device. The second connection interface including a secondary connection port for communicatively coupling to a downstream network device via a wireless technology. In one exemplary implementation the second connection interface is adapted to be secured in a fixed location while conveniently providing the communicative coupling to a downstream network device via a wireless technology. The means for intelligently concentrating data concentrates data from a plurality of interface connection ports included in the second connection interface for communication on the primary connection port of the first connection interface. The communication bus communicatively couples the first connection interface to the second connection interface.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1A is a block diagram of a LAN with one embodiment of a present invention multi-configuration network connection point device.

Figure 1B is a block diagram of another LAN, one exemplary implementation of the present invention in which multi-configuration network connection point devices are coupled to each other.

Figure 2A is a block diagram of multi-configuration network connection point device, one embodiment of the present invention.

Figure 2B is a block diagram of another embodiment of a present invention multi-configuration network connection point device.

Figure 3 is a block diagram of an intelligent concentrator, one implementation of a present invention multi-configuration network connection point device.

Figure 4 illustrates a possible configuration for a secondary connection interface in one embodiment of the present invention.

Figure 53 is a flow chart of a multi-configuration network connection point method, one embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Reference will now be made in detail to the preferred embodiments of the invention, a network access intelligent concentrator device and method, examples of which are illustrated in the accompanying drawings. While the invention will be described in conjunction with the preferred embodiments, it will be understood that they are not intended to limit the invention to these embodiments. On the contrary, the invention is intended to cover alternatives, modifications and equivalents, which may be included within the spirit and scope of the invention as defined by the appended claims. Furthermore, in the following detailed description of the present invention, numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will be obvious to one ordinarily skilled in the art that the present invention may be practiced without these specific details. In other instances, well known methods, procedures, components, and circuits have not been described in detail as not to unnecessarily obscure aspects of the current invention.

NOTATION AND NOMENCLATURE

Some portions of the detailed descriptions which follow are presented in terms of procedures, steps, logic blocks, processing, and other symbolic representations of operations on data bits that can be performed on computer

memory. These descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. A procedure, computer executed step, logic block, process, etc., is here, and generally, conceived to be a self-consistent sequence of steps or instructions leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated in a computer system. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussions, it is appreciated that throughout the present invention, discussions utilizing terms such as "processing" or "computing" or "translating" or "calculating" or "determining" or "scrolling" or "displaying" or "recognizing" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within

the computer system memories or registers or other such information storage, transmission or display devices.

Figure 1 is a block diagram of LAN 100A with one embodiment of a present invention multi-configuration network connection point device. LAN 100A comprises a server 175, work groups 110, 120 and 130 and multi-configuration network connection point devices 101, 102, and 103. The plurality of work groups 110, 120 and 130 are communicatively coupled to the LAN by multi-configuration network connection point devices 101, 102, and 103, respectively. Multi-configuration network connection point devices 101, 102, and 103 each include a primary connection interface with a single communication port and a secondary connection interface with a plurality of communication ports. Multi-configuration network connection point devices 101, 102, and 103 are communicatively coupled to upstream communication devices (e.g., server 175) by single communication paths 119, 129 and 139 respectively. Work groups coupled to LAN 100A can take a variety of configurations and components included in the work groups can perform a variety of functions. For example, work group 110 comprises wireless device 111, work station 112 (e.g., a personal computer) work station 113, work group 120 comprises a work station 121, peripheral device 122 (e.g., a printer), and wireless device 123; and work group 130 comprises wireless device 131 (e.g., a telephone, personal computer, laptop, personal digital assistant, etc.) LAN 100A is coupled to WAN 185 and power supply 145.

Each of the devices included in LAN 100A requires a communication network connection point to communicate with other devices coupled to LAN 100A. Multi-configuration network connection point devices 101, 102, and 103 provide a convenient efficient communication network connection point for the end use devices (e.g., between devices within the same work group, between devices in different work groups, between end use devices and upstream devices, etc). The multi-configuration network connection point devices are readily adaptable for providing a network connection point for a variety of devices utilizing different communication protocols and the primary connection interface single port does not require separate parallel cable runs to couple with upstream devices. In one embodiment of the present invention, multi-configuration network connection point devices 101, 102, and 103 are configured for anchored placement in fixed locations (e.g., recessed in a wall or office cubicle section) in a manner that facilitates maintenance of system integrity and security.

Figure 1B is a block diagram of LAN 100B, one exemplary implementation of the present invention in which multi-configuration network connection point devices are coupled to each other. LAN 100B is similar to LAN 100A except multi-configuration network connection point devices 101, 102, and 103 are communicatively coupled to upstream communication devices by serial communication paths 118, 128 and 138

respectively (e.g., in a daisy chain fashion). Communications from downstream multi-configuration network connection point devices are passed through to upstream devices.

In one embodiment of the present invention, network connection point devices 101, 102 and 103 facilitate wireless communication to end use devices. In one exemplary implementation network connection point devices 101, 102 and 103 provide an interface for wireless communications to downstream devices and hardwired communications to upstream devices. In one embodiment of the present invention, network connection point devices 101, 102 and 103 are capable of "seamlessly" handing off of communication connections as an end use device moves between work groups. In one exemplary implementation, wireless device 123 initiates a communication with server 175 via multi-configuration network connection point devices 102 and seamlessly continue the communication via multi-configuration network connection point devices 103 (e.g., as wireless device 123 is moved from work group 102 area to work group 103 area).

Figure 2A is a block diagram of multi-configuration network connection point device 200A, one embodiment of the present invention. Multi-configuration network connection point device 200A comprises a primary connection interface 210 and a secondary connection interface 220. In one embodiment of the present invention, primary connection interface 210

is communicatively coupled to upstream network devices and secondary connection interface 220[3] is communicatively coupled to downstream network devices. In one embodiment of the present invention, primary connection interface 210[3] comprises primary connection interface port 211[3]. In one embodiment of the present invention, secondary connection interface 220[3] comprises a first secondary connection interface port 221[3], a second secondary connection interface port 222[3], a third secondary connection interface port 223[3], and a fourth secondary connection interface port 224[3]. Multi-configuration network connection point device 200A[3] is readily adaptable for anchored placement in fixed locations (e.g., recessed in a wall or office cubicle partition).

The components of multi-configuration network connection point device 200A[3] cooperatively operate to communicatively couple devices via the primary connection interface and the secondary connection interface. In one embodiment of the present invention, the secondary connection interface utilizes wireless technology to communicate with end use devices. In one exemplary implementation of the present invention, a secondary connection interface port (e.g., 221[3]) includes a wireless communication component for facilitating wireless communications. The wireless communication component includes an antenna for propagating electromagnetic communication signals, a transmitter for transmitting the electromagnetic signals and a receiver for receiving the electromagnetic signals.

It should be appreciated that the present embodiment is not meant to limit the possible number of connection ports included in an interface of a multi-configuration network connection point device. While a preferred embodiment of the present invention includes a plurality of connection ports on one interface and a single connection port on the other to take advantage of singular communication path (e.g., cable run) to an upstream device, the present invention is readily adaptable to a provide a variety of additional features (such as security, fault detection etc.) that are applicable to a plurality of connection ports on each interface.

Figure 2B[3] is a block diagram of multi-configuration network connection point device 200B[3], one embodiment of the present invention. In one embodiment of the present invention, multi-configuration network connection point device 200B[3] intelligently concentrates and distributes communications between a plurality of interface connection ports and a single interface connection port. In one exemplary implementation, data communicated via multi-configuration network connection point device 200B[3] is multiplexed and demultiplexed between a plurality of secondary connection interface ports and a single primary connection interface port. In one embodiment of the present invention, a multi-configuration network connection point device comprises intelligent connection determination means 250[3] for processing and interpreting data communicated via multi-configuration network connection point device 200B[3] to determine

appropriate connection configurations. In one exemplary implementation of the present invention, the intelligent connection determination means 250[3] includes a central processing unit (CPU) and a random access memory (RAM). The intelligent connection means processes and interprets data to provide a number of functions, including intelligent routing of data, security measures, maintenance and troubleshooting features, etc.

In one embodiment of the present invention a multi-configuration network connection point device includes a fault detection means 270[3] coupled to the intelligent connection determination means 250[3] for processing and interpreting data. It is appreciated that fault detection means 270[3] may be implemented in a variety of embodiments including but not limited to a hardware fault detector, a fault detection circuit, a software fault detector, a link beat signal fault detector, a ping signal fault detector, a loop-back mode for fault detection, etc. In one embodiment, fault detection means 270[3] (e.g., hardware, software, firmware, etc.) participates in fault detection operations in a communication network and is utilized to facilitate fault isolation in a network. In one embodiment, fault detection means 270[3] operates in conjunction with a head end component of a network in the performance of fault detection activities.

Figure 3[3] is a block diagram of intelligent concentrator 301[3], one implementation of a present invention multi-configuration network

connection point device. Intelligent concentrator 301 is shown in a side cutaway view, with secondary connection interface ports 304 (e.g., connection jacks) and wireless component 307 shown in one of several conceivable arrangements. Wireless communication component 307 is readily adaptable for implementation in a variety of protocols, including infrared or radio frequency (e.g., bluetooth) implementations. In one exemplary implementation of the present invention, multiplexing/demultiplexing of signals to and from a server is under the control of in-unit electronics 302. Again, communication signals and possible power travel over single cable 330 and connect to intelligent concentrator 301 via primary connection interface port connector 306. Anchoring means 309 fastens intelligent concentrator 301 to a stationary member (e.g., a wall, office cubicle section, floor, ceiling, etc.). Anchoring means 309 is readily adaptable to a variety of implementations including but not limited to, bolt, clamp, hook, latch, lock, lug nail, nut, pin, rivet, screw, etc. In one implementation of the present invention, anchoring means 309 is adapted to fasten intelligent concentrator 301 so portions of intelligent concentrator 301 behind anchoring plate 320 towards primary connection interface port connector 306 are recessed in a cavity of a stationary member.

Also shown in Figure 3 is add-on device 303 that is coupled to intelligent concentrator 301. A range of possibilities exists for the functions of device 303. It could be implemented as an intelligent remote testing device,

allowing the network infrastructure and cabling to be tested and evaluated from a central location, without any action being required at the work site. Device 303 might also be implemented as a security device, preventing physical attachment to the LAN cabling without a notification being sent to the server that the physical network port has been compromised. In one embodiment of the present invention, wireless component 307 in included in add-on device 303 and provides wireless communication capabilities to an embodiment of a present invention intelligent concentrators that does not have integrated wireless communication capabilities.

Figure 4 illustrates a possible configuration for a secondary connection interface in one embodiment of the present invention. Intelligent concentrator 301 is shown here with a secondary connection interface comprising four RJ-45 jacks 304. In one embodiment there is additional space for additional jacks 308, even when the configuration of intelligent concentrator 301 is adapted to covering a space similar to a standard wall plate device. In one embodiment of the present invention, a secondary connection interface includes a connection to a different network or to a telephone system. Figure 4 also shows an embodiment of the present invention with a status indicator light 305 for providing a conveniently observable status indication.

Also shown in Figure 4 is wireless communication component 307. Wireless communication component 307 could be implemented in any number of wireless standards for a communication connection without a fixed physical tether to other network devices. In one embodiment of the present invention, necessary transceiver electronics for device 307 are included within in the body of concentrator 301 (e.g., integral with internal electronics 302).

In one exemplary implementation of the present invention, wireless signals transmitted from a present invention multi-configuration network connection point device have a very short range. For example, a multi-configuration network connection point device transmits signals that are directed to a specific area (e.g., a work area) and/or are very low power communication signals that rapidly attenuate beyond a predetermined range (e.g., 10 feet). These short range transmissions are implemented in a manner that makes illicit interception from distant wireless devices (e.g., outside the location of a work area) very difficult. In one embodiment of the present invention, multi-configuration network connection point device is adapted to participate in encrypted communications, including requiring reception of an encrypted code before granting access to a communications network via the multi-configuration network connection point device. In one embodiment of the present invention, multi-configuration network connection point device imposes a vicinity test (e.g., a motion detector, finger

print detector, sound detector, keypad detector, etc.) before being granted access to a communication network.

In one embodiment of the present invention, a multi-configuration network connection point device is adapted to receive power and forward it to downstream devices. In one exemplary implementation of the present invention, a multi-configuration network connection point device is adapted to receive power via a single primary interface port (e.g., 211) and forward it via a plurality of secondary interface ports (e.g., 221, 222, 223, and 224). In another exemplary implementation of the present invention, a multi-configuration network connection point device is adapted to receive and/or forward power via dedicated interface ports (e.g., coupled to a separate dedicated power cable). In one embodiment of the present invention, a multi-configuration network connection point device provides power management functions. In one exemplary implementation of the present invention, a multi-configuration network connection point device intelligent connection means controls on, off and low power modes. For example, a multi-configuration network connection point device switches between power modes based upon activity in a location (e.g., motion in a room), on the network (e.g., no data traffic communicated via the multi-configuration network connection point device for a period of time), time of day, etc.

The present invention facilitates power connections in a manner that assist isolating the effects of electrical faults (e.g., due to component failures or shorts in a connected devices or the wires leading to the connected device). For example, a multi-configuration network connection point device is configured to prevent external failures (e.g., faults, short circuit, etc.) from damaging or impacting the multi-configuration network connection point device itself, or other external components via the multi-configuration network connection point device. In one embodiment of the present invention, a multi-configuration network connection point device provides operational recovery at an affected port as soon as a failed external device or wire is unconnected (e.g., with current limiting fold back circuitry), self healing "poly switch" fuses). In one embodiment of the present invention, embedded intelligence (e.g., intelligent connection means 250) sense a failure or fault condition and issues a signal reporting the failure or fault (e.g., to a central management device).

Figure 5 is a flow chart of multi-configuration network connection point method 500, one embodiment of the present invention.

In step 510, a single connection point on a primary communication interface is provided. In one embodiment of the present invention the single connection point couples to a single communication path (e.g., to upstream network devices). In one embodiment of the present invention, the single

connection point is configured for fixed placement in a concealed environment.

In step 520 a plurality of connection points on a secondary communication interface is provided. In one embodiment of the present invention the secondary communication interface is adapted to be secured in a fixed location while conveniently providing said communicatively coupling to a downstream network device via a wireless technology.

In step 530 the single connection point on a primary communication interface is coupled to the plurality of connection points on a secondary communication interface. In one embodiment of the present invention intelligently concentrating data from a plurality of interface connection ports included of said second connection interface for communication on said primary connection port of a first connection interface.

Thus, the present invention is a system and method that facilitates convenient connection to a communication network. A present invention multi-configuration network connection point device enables wireless devices to connect to a communication network. The "tamper" proof interface and recessed components of a multi-configuration network connection point device facilitates network maintenance and troubleshooting. The characteristics of the wireless communications and

sensory capabilities of the multi-configuration network connection point device provide added security capabilities for network communications.

The foregoing descriptions of specific embodiments of the present invention have been presented for purposes of illustration and description. They are not intended to be exhaustive or to limit the invention to the precise forms disclosed, and obviously many modifications and variations are possible in light of the above teaching. The embodiments were chosen and described in order to best explain the principles of the invention and its practical application, to thereby enable others skilled in the art to best utilize the invention and various embodiments with various modifications as are suited to the particular use contemplated. It is intended that the scope of the invention be defined by the Claims appended hereto and their equivalents.

SECTION 4

The present invention relates to an apparatus for multiplexing signals in a network. The apparatus has a housing which contains two or more network connection devices along with suitable intelligent electronic circuitry for controlling and multiplexing data, voice telephone signals, and power for multiple devices connected to the connection devices. The multiplexing enables the various devices to communicate with the network and, in some cases, to receive power over the network connection. The intelligent electronic circuitry is also capable of aiding in network security and management and in power management. The intelligent electronic circuitry is powered by network-delivered device power. A primary advantage of the disclosed invention is an enormous reduction in the network cabling required for a new network installation, a near elimination of the need to install new cabling for modification of an existing network, and much enhanced reliability and manageability of the network.

SECTION 4

This Section 4 relates to the field of Local Area Networking (LAN). More specifically, this Section 4 relates to a device and system for efficiently multiplexing data, voice and power lines between the work site and the network.

BACKGROUND

Modern Local Area Networking (LAN) is generally accomplished by extensive runs of multiple parallel cables to multiple connections and devices at each work site. This is in addition to voice telephone and utility power cabling for devices. When LAN infrastructures require change, it is generally more efficient to leave existing cables in place and simply string new cables between switch and router nodes and any new work site devices.

The current state of the art for implementing utility power for devices associated with a LAN, both computers and peripherals, is centered around providing a large number of general purpose AC outlets in the vicinity of the computing equipment that is to be connected to a data LAN. Current distributed solutions are ad hoc, of questionable reliability, inefficiently managed and subject to failures caused by accidental removal of power and wire breakage.

Current solutions require local power which adds an installation requirement and reduces system reliability. Security and safety of data in a network can also be jeopardized by uncontrolled access to utility power in a work center. Security could be further bolstered by controlling access to power in the same manner and system as controls data security.

What is needed, then, is a means of reliably supplying power in a system that multiplexes voice and data lines in order to reduce the cost of installation and infrastructure change in a LAN. Furthermore, power must also be supplied via the connection jack to operate peripheral devices at the work center and securely and reliably supply power to operate the intelligent circuitry of the intelligent connection device itself.

SUMMARY

Presented herein is a means for reliably supplying power to an intelligent local area network connection jack that reliably multiplexes voice, data and power lines in order to reduce the cost of installation and infrastructure change in a LAN. Furthermore, the power is supplied via the connection jack to also operate peripheral devices at the work center and can securely and reliably supply power to operate the intelligent circuitry of an intelligent connection device.

The present invention relates to an apparatus for multiplexing signals in a network. The apparatus has a housing which contains two or more network connection devices along with suitable intelligent electronic circuitry for controlling and multiplexing data, voice telephone signals, and power for multiple devices connected to the connection devices. The multiplexing enables the various devices to communicate with the network and, in some cases, to receive power over the network connection. The intelligent electronic circuitry is also capable of aiding in network security and management and in power management. The intelligent electronic circuitry is powered by network delivered device power. A primary advantage of the disclosed invention is an enormous

reduction in the network cabling required for a new network installation, a near elimination of the need to install new cabling for modification of an existing network, and much enhanced reliability and manageability of the network.

These and other objects and advantages of the present invention will become obvious to those of ordinary skill in the art after having read the following detailed description of the preferred embodiments which are illustrated in the various drawing figures.

BRIEF DESCRIPTION OF THE DRAWINGS

The operation of this invention can be best visualized by reference to the drawings.

Figure 1 (Prior art) illustrates a conventional LAN implemented with a server and work centers.

Figure 2A illustrates a LAN, configured in accordance with one embodiment of the present invention.

Figure 2B illustrates a variation on a LAN equipped with embodiments of the present invention.

Figure 3 illustrates a block diagram of an exemplary connection of an intelligent connection apparatus in accordance with one embodiment of the present invention.

Figure 4A illustrates a possible configuration for one embodiment of the present invention.

Figure 4B illustrates another possible configuration for one embodiment of the present invention.

Figure 5 illustrates a block flow diagram of one embodiment of the present invention.

BEST MODE FOR CARRYING OUT THE INVENTION

Reference would now be made in detail to the preferred embodiments of the invention, examples of which are illustrated in the accompanying drawings. While the invention will be described in conjunction with the preferred embodiments, it will be understood that they are not intended to limit the invention to these embodiments. On the contrary, the invention is intended to cover alternatives, modifications and equivalents, which may be included within the spirit and scope of the invention as defined by the appended claims. Furthermore, in the following detailed description of the present invention, numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will be obvious to one of ordinary skill in the art that the present invention may be practiced without these specific details. In other instances, well-known methods, procedures, components, and circuits have not been described in detail so as not to unnecessarily obscure aspects of the present invention.

Some portions of the detailed descriptions that follow are presented in terms of procedures, logic blocks, processing, and other symbolic representations of operations on signals within an electronic circuit. These descriptions and representations are the

means used by those skilled in the electronic arts to most effectively convey the substance of their work to others skilled in the art. A procedure, logic block, process, etc., is here, and generally, conceived to be a self-consistent sequence of steps or instructions leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated in an electronic system.

There are many conceivable embodiments of the present invention. However, the concepts underlying the present invention may be best understood by the discussion of only a few embodiments. This discussion in no way limits the application of the concepts nor determines the limit to embodiments possible.

Enhanced understanding of the concepts presented in this discussion of this embodiment of the present invention may be had by reference to the attached Figures.

Prior art Figure 1 illustrates a conventional LAN implemented with a server and three work centers, such as illustrated at 110. A work center might be populated with a workstation 107, a network

printer 108, a laptop 101 or other devices and combinations of devices that require direct communication with the server in order to function properly. Additionally, a voice telephone, 109, using Voice Over Internet Protocol (VOIP) technology might be in the modern workplace. Each of these devices requires a cable connection to the server 104, which also in this illustration supplies connectivity to the internet at 103, or to its peripheral switching mechanisms. As discussed earlier, each of these connections currently requires a separate cable run for data, 100, and another for power, 120, which can be very expensive and can compromise system integrity and security.

Work center devices generally require electrical power to operate and that power is normally supplied by utility 120 VAC (volts, alternating current) electrical outlets. Some modern devices, such as scanners, printers, voice phones and other computer peripherals, actually require a lower voltage DC (direct current) power source and obtain it by converting utility power to the required level prior to its use. No matter the final character of power used, utility power accessed in the modern work center is a completely separate system from the data network and is subject to different operating rules and control.

The embodiment of the present invention discussed here implements device power in the same intelligent hardware that can be used to provide a centralized data network connection: an intelligent concentrator. By supplying power connection through the same device as data connection, an additional source of network security can be had and a significant reduction in facility wiring costs can be obtained.

Figure 2A[4] illustrates a LAN, configured with the same equipment as in Figure 1[4], where the work area equipment has been connected to the network via the network connection apparatus, at the seat of embodiments of the present invention, which can be called intelligent concentrator or smart network portal, 200[4]. All of the same functions and devices of the previous work centers are represented but, using an intelligent concentrator, a single cable is all that is required to connect the work area equipment suite with the server. VOIP telephone 109[4] is implemented as well in the equipment array.

Also illustrated in Figure 2A[4] is one implementation of device power over the network connection. In this case, device power 220[4] is multiplexed onto device data cables 100[4] as shown. This can be implemented for devices whose power requirements are low enough

to make such a multiplexed power supply system cost effective. A high power requirement can drive the cable sizes too large to make any cost savings be attainable. In that case power can still be supplied through the connection apparatus but by use of a separate cable. By connecting power through the intelligent concentrator, monitoring and control of power can still be implemented.

Figure 2B[4] illustrates a variation on the LAN equipped with intelligent concentrators. Here, a further reduction in cabling cost is gained by the use of a "daisy-chained" arrangement of intelligent concentrators, 200[4]. A daisy-chain would result in only one cable being connected directly to the server 104[4], or to its peripheral switching center, to connect a plurality of work centers. As in the illustration in Figure 2A[4], power 220[4] is again multiplexed over network data cables, 100[4]. It must be noted here that power supplied to the intelligent circuitry of an intelligent concentrator can normally be supplied by multiplexing on data cabling between the server and the concentrator. This is the case even when power is supplied to the work center devices by parallel cabling.

An intelligent concentrator is easy to install and reliably provides an attachment point for access to Voice & Data Networks. The embodiment of the present invention discussed here is

implemented through miniaturized hardware that could be installed inside a wall or in an internal space provided for in an office cubicle. Power is easily supplied using the same hardware. Access to device power is simultaneously accessible with data line connection.

Note here that Figures 3, 4A and 4B illustrate a form factor for intelligent concentrator 200 that is similar to a U.S. standard utility wall plate. This illustration is only meant for illustration. There are any number of standard form factors in which this embodiment of the present invention can be implemented without impacting its functionality and utility.

Figure 3 illustrates a possible configuration for an embodiment of the present invention. Intelligent concentrator 200 is shown in side cutaway view, with connector jacks 304 and wireless communication device 307 shown in one of several possible arrangements. A possible wireless communication device 307 is envisioned as being enabled in a variety of protocols. Multiplexing of signals and power to and from server 104 would very likely be under the control of in-unit electronics 302. Again, those signals and power for some devices would be multiplexed onto single cable 100 and connect to intelligent concentrator 200 via back-of-unit

connector 306. Power to server 104 or to its switching center, is illustrated by utility power cable 221. Note here that, while embodiments of the present invention may use low voltage DC power for reasons of safety and noise considerations, other embodiments may provide and monitor other power protocols, including 120 VAC utility power.

Also shown in Figure 3 is add-on device 303. A range of possibilities exists for the functions of device 303. It can be implemented as an intelligent remote testing device, allowing the network infrastructure and cabling to be tested and evaluated from a central location, without any action being required at the work site. Device 303 can also be implemented as a security device, preventing physical attachment to the LAN cabling without a notification being sent to the server that the physical network port has been compromised. Device 303 can receive its power via the same multiplexed cabling as does intelligent circuitry 302.

In one embodiment, several standard communications jacks, such as RJ45, as well as status indicator lights, are mounted on the external, user accessible, surface of the intelligent concentrator. This embodiment of the present invention provides for low voltage DC device power to be supplied directly through one of the several

RJ-45 communication jacks. However, alternative implementations, such as USB or even a utility AC socket could support power connections.

Connections to the central data network (LAN) and to power in the present embodiment are terminated at the connection apparatus. These connections are established by an installer and are be intended to be accessible by the end user. In most instances, the wiring between the unit and the communications and power infrastructure terminate inside the wall or possibly office cubicle fixture. Termination of the network wiring (voice or data) provides for both a reliable electrical and mechanical connection for industry standard communications cabling such as CAT3, CAT5 or CAT5E or similar cabling. In another embodiment, electrical power is supplied by parallel wiring installed coincident to the installation of the data cabling. It is envisioned that the integrity of the installation may utilize mounting hardware such as screws or snap fit techniques that could not removed by an end user without specialized tools.

Figure 4A illustrates a possible configuration for an embodiment of the present invention. Intelligent concentrator 200 is shown here with four RJ-45 jacks, 304. There is space, even if an intelligent concentrator takes the form factor of a standard wall

plate device, for more jacks, 308[4]. These other jacks could enable a parallel connection to a different network or to a telephone system or to a number of other envisioned possibilities. Figure 4A[4] also shows status indicator light 305[4] which could be implemented in one embodiment. In this implementation, peripheral device power would be supplied by multiplexed power over data cabling and would be present in the RJ-45 connectors illustrated. A wide variety of other connectors and protocols could also be accommodated by the same scheme.

Also shown in Figure 4A[4] is wireless communication device 307[4]. Device 307[4] could be implemented in any number of wireless standards for non contact connection to the network. The necessary transceiver electronics for device 307[4] can be contained in the body of intelligent concentrator 200[4], and can be integral with internal electronics 302[4]. Power for communications device 307[4] and its associated circuitry can, like intelligent electronic circuitry 302[4] and device 303[4], be received via multiplexed cabling.

In addition to terminating data connections, this embodiment of the present invention supports device power supplies. In the one implementation, an RJ-45 connector or other modular connector is configured to provide both a data connection and a power connection

for some types of devices. The end user inserts a data cable or a telephone into the jack and either device would be supported. The end user would not have to actively configure or program this embodiment to enable either mode of operation. For devices demanding power that isn't suitable for support in an RJ-45, an additional connection can be offered.

In addition to wired connections to and from this embodiment and the client devices, wireless connectivity is also supported by the intelligent concentrator. In an embodiment using wireless connectivity, it is likely that a wireless device can operate on battery power. Then a means is supplied that will enable battery charging through the intelligent concentrator.

To enable wireless connectivity, an antenna or an IR port, illustrated at 307[4] in Figure 3[4], can be built into the face of the implemented unit itself. The antenna can also be constructed to allow it to be implemented on or above the surface and can be implemented in some embodiments as an extendable antenna and even as a separate antenna connected by cable. The electronics suite contained within the housing in this embodiment can provide the additional supporting circuitry to implement a wireless connection.

Figure 4B illustrates a slightly different device power scheme. Here utility socket 320 is shown in order to illustrate the application of high voltage or current power that reaches the intelligent concentrator via parallel cabling. With access to the power being through intelligent concentrator 200, management and control of the power supply can still be maintained even though the electrical power is carried over lines other than those carrying data. The illustration of a utility power socket is not meant to imply that there is some special application of 120 VAC power in this embodiment. The illustration is solely meant to illustrate a parallel application of power through the device as opposed to power supplied via a connector such as an RJ-45. Any number of power protocols can be used in various embodiments.

Figure 5 illustrates a block flow diagram of one embodiment of the present invention. There, in process 500, an intelligent concentrator is provided at 510 for each applicable network work center. Network devices, such as computers and peripherals, are connected at 520 and electrical power is supplied for both the intelligent concentrator and the connected network devices at 530. At 540, applicable data, VOIP signals, and electrical power are multiplexed over the installed network cabling or parallel power

cabling. Power is monitored and controlled at 550 and the process ends, when terminated, at 599.

Power for the embodiment of the present invention discussed here, as well as devices connected to it, is provided from a central source over the network cabling or in dedicated power cables installed at the same initial installation. Control over power supplied to the concentrator and forwarded by it to the connected devices can then be maintained in the network management infrastructure. The power that is provided can be connected in a manner that would also isolate the effect of electrical faults due to component failures or shorts in the connected devices or the wires to them. Such isolation prevents a failure that is external to this embodiment from damaging it and can isolate the failure in a way that will allow the implementation of this embodiment and devices that are connected to the unit to remain operational. Recovery of the effected port can be automatic and can occur as soon as the failed device or wire is removed. This embodiment implements this feature with current limiting fold back circuitry. This embodiment also allows the embedded intelligence to sense the condition and report it to a central management console. An alternative implementation could be through self-healing "Poly Switch" fuses.

The benefits that accrue from combining power supply and data connection in the same physical device in the manner already described add significantly to the functionality, reliability and the range of functions that can be performed by this embodiment. Installations that do not provide for the termination of the wiring to the network internal to a protected surface such as a wall or a cubicle are inherently unreliable and are subject to a degrading of connections from mechanical stress, abrasion and related mechanisms. Degrading of electrical power cabling can lead to expensive power outages if not a fire hazard. The placement of attachment points in a protected environment can eliminate problems from accidental stresses that could occur. Mechanical stress can occur if a user snares a device cable and inadvertently pulls on the embodiment, either directly or through the attached cable. The mounting hardware can isolate the forces to which the wiring is subjected.

Another benefit of the physical attributes of the embodiment that has been described is that the end user does not have direct access to the network infrastructure. This embodiment of the present invention itself can serve as a managed access control point. If this embodiment is established in another manner such as a stand

alone box, the end user might be able to circumvent the functions performed by this embodiment and gain direct, unmanaged, access to the network. It is apparent that concepts presented in this embodiment of the present invention provide an added degree of security by presenting a controlled point of access.

A significant advantage, offered by the embodiments of the present invention employing RF communication, is the provision of a degree of directionality that can optimized to limit the number of devices, both intended and unintended, with which any unit is able to communicate. By employing directionality and shielding, the occupant of a workspace is able to reliably communicate with the unit while another person in an adjacent space using similar equipment is less likely to interfere with or even gain access to the first user's communication.

In one embodiment, the unit is produced as separate elements. The base unit contains the capability to terminate the cabling while a separate unit containing the intelligent electronics is added to the base unit at a later time. The functional split of the unit in this manner allows for wide deployment of network wiring infrastructure in a cost effective manner since the cost of the intelligence is not borne for work areas that might not currently be

occupied. Other benefits that derive from this type of functional partitioning is in the area of field service and upgrades. A unit that is suspected to have failed can quickly be replaced and retested. Also, newer units with added capabilities can be added where needed and older modules can still be used in areas where the added capabilities are not needed.

In yet another embodiment, a modular expansion capability is added onto the base unit to enable the functions of the deployed units to be readily adopted to new and varying needs. The expansion module can mate onto the faceplate and can obtain bus signal and power from it. Serial buses such as USB or Ethernet can be suitable for this purpose. The implementation of a modular add-on could be implemented in a fashion so the end user would not view the bus expansion connector as a general purpose interface as is often the case with a PC. This can be done to avoid problems that could arise if end users inserted cables directly into industry standard expansion connectors, expecting to enable the functions provided by a peripheral device. There also would not necessarily be an easy means to add the required software elements nor a user interface to support the level of communications with an end user that some peripherals require.

Some implementations of this embodiment of the present invention are plug-in add-ons that securely mount over existing data communications jacks. An alternative mounting technique for this embodiment can be to allow the unit to mount over and plug into the existing communication jacks.

The wall mounted units can provide for additional capabilities such as data concentration, security, VOIP support, etc. However, to achieve the real benefits of the added reliability and security similar to what was described for in wall mounting, the attachment needs to be implemented in a manner that enables for a quick and easy installation while providing for a capture mechanism that is not releasable by the end user.

The foregoing descriptions of specific embodiments of the present invention have been presented for purposes of illustration and description. They are not intended to be exhaustive or to limit the invention to the precise forms disclosed, and obviously many modifications and variations are possible in light of the above teaching. The embodiments were chosen and described in order to best explain the principles of the invention and its practical application, to thereby enable others skilled in the art to best utilize the invention and various embodiments with various

modifications as are suited to the particular use contemplated. It is intended that the scope of the invention be defined by the Claims appended hereto and their equivalents.

SECTION 5

A method and device for power management of intelligent hardware (e.g., an intelligent data concentrator) for providing access to voice and data networks. Power use data of the intelligent hardware is obtained, wherein the intelligent hardware is coupled to a power source and communicatively coupled to a voice or data network. The intelligent hardware is configured to communicatively couple a plurality of electronic devices to the network. Using the power use data, a power mode of the intelligent hardware is determined. In one embodiment, the present invention comprises a first interface for communicatively coupling the intelligent hardware to the network and a power source and a second interface for communicatively coupling the intelligent device to the plurality of client devices. The intelligent device also comprises means for processing and interpreting data coupled to the first interface, and power mode control means coupled to the means for processing and interpreting data. In one embodiment, the power mode control means is configured to obtain the power use data of the intelligent hardware and is configured to use the power use data to determine a power mode of the intelligent hardware.

SECTION 5

This Section 5 relates to the field of computer networks. In particular, this Section 5 relates to a method for power management of intelligent hardware for providing access to voice and data networks.

BACKGROUND

In a large number of working environments, people use a large number of electronic devices connected to a network to perform the duties of their jobs. Any one person may have several electronic devices located within their personal area network (PAN). For example, these electronic devices may include a computer system, a voice IP telephone and a printer.

Currently, a growing concern of businesses is the increasing cost of power. Often, electronic devices are turned on, and thus consume power, even if they are not in use. For example, an electronic device may remain turned on after business hours, over the weekend or holidays, or in an empty office or cubicle. Often, this is simply due to human forgetfulness. However, the cost of paying for the use of these electronic devices, particularly in large corporations with thousands of electronic devices, can be very high. Presently, this concern is of great importance not only to those footing the bill for the power consumption, but those persons not able to get power due to the consumption of unused electronic devices (e.g., resulting in a blackout).

Often, if an electronic device is not manually powered off or placed in a low power mode, the electronic device will continue to consume power at its typical rate. While, some electronic devices may be programmed to be powered off or placed in a low power mode automatically (e.g., sleep mode of a computer system), there is currently no way to change the power mode of all devices in a PAN based on detected activity or predetermined criteria.

In most situations, electronic devices are coupled to a network through a simple router or hub, and the activity of the electronic device cannot be easily monitored. Furthermore, most electronic devices receive power from an independent power source distinct from the network. As a result, there us currently no way to detect the power usage of electronic devices in a PAN, and to adjust their power mode accordingly.

A need exists for a method and a device thereof for detecting the level of activity of electronic devices in a PAN. A need also exists for a method and a device thereof for automatically turning off the electronic devices or placing the electronic devices in a low power mode when they are not being used or according to predefined criteria. Particularly, a need exists for a method and a device thereof for managing the power mode of electronic devices in a PAN.

SUMMARY

Accordingly, the present invention provides a method and a device thereof for detecting the level of activity of electronic devices in a PAN. The present invention also provides a method and a device thereof for automatically turning off the electronic devices or placing the electronic devices in a low power mode when they are not being used or according to predefined criteria. The present invention also provides a method and a device thereof for managing the power mode of electronic devices in a PAN.

A method and device for power management of intelligent hardware (e.g., an intelligent data concentrator) for providing access to voice and data networks is presented. Power use data of the intelligent hardware is obtained, wherein the intelligent hardware is coupled to a power source and communicatively coupled to a voice or data network. The intelligent hardware is configured to communicatively couple a plurality of electronic devices to the network. Using the power use data, a power mode of the intelligent hardware is determined.

In one embodiment, the present invention comprises a first interface for communicatively coupling the intelligent hardware to the network and a power source and a second interface for communicatively coupling the intelligent device to the plurality of client devices. The intelligent device also comprises means for processing and interpreting data (e.g., a processor) coupled to the

first interface, and power mode control means coupled to the means for processing and interpreting data. In one embodiment, the power mode control means is configured to obtain the power use data of the intelligent hardware and is configured to use the power use data to determine a power mode of the intelligent hardware.

In one embodiment, the intelligent hardware is communicatively coupled over the network to a central control site, wherein the power use data is defined at the central control site. In another embodiment, the power use data is predefined and stored in intelligence of the intelligent hardware. In one embodiment, the power use data is user-defined.

In one embodiment, the power use data is obtained by detecting a level of activity of the intelligent hardware (e.g., data transfer through the intelligent hardware). In another embodiment, the power use data is obtained by detecting a level of activity within a predetermined area containing the intelligent hardware. The level of activity may be detected by a variety of sensors, including but not limited to a motion detector, a heat sensor or a sound detector.

In one embodiment, the present invention provides a method and device for automatically turning an intelligent data concentrator off or placing an intelligent data concentrator into a low power mode. In one embodiment, the

low power mode or off mode is activated based on the time of day, week, or year. In one embodiment, the intelligent hardware is configured to supply power from the power source to the plurality of electronic devices. In one embodiment, changing the power mode if the intelligent hardware operates to change the power of mode to each electronic device coupled to receive power through the intelligent hardware.

These and other objects and advantages of the present invention will become obvious to those of ordinary skill in the art after having read the following detailed description of the preferred embodiments which are illustrated in the various drawing figures.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and form a part of this specification, illustrate embodiments of the invention and, together with the description, serve to explain the principles of the invention:

FIGURE 1 illustrates an exemplary wired desktop cluster coupled to a local area network (LAN) in accordance with one embodiment of the present invention.

FIGURE 2 is a block diagram of a cross-sectional view of an intelligent data concentrator in accordance with one embodiment of the present invention.

FIGURE 3 is an illustration of a perspective view of an exemplary faceplate of an intelligent data concentrator in accordance with one embodiment of the present invention.

FIGURE 4 is a block diagram of an exemplary LAN upon which embodiments of the present invention may be practiced.

FIGURE 5 is a flowchart diagram of the steps in a process for power management of intelligent hardware (e.g., an intelligent data concentrator) for

providing access to voice and data networks in accordance with one embodiment of the present invention.

FIGURE 5 is a block diagram of an intelligent data concentrator configured for performing a process of power management in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION

In the following detailed description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that the present invention may be practiced without these specific details. In other instances, well-known structures and devices are not described in detail in order to avoid obscuring aspects of the present invention.

Some portions of the detailed descriptions which follow are presented in terms of procedures, steps, logic blocks, processing, and other symbolic representations of operations on data bits within a computer memory. These descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. A procedure, computer executed step, logic block, process, etc., is here and generally conceived to be a self-consistent sequence of steps of instructions leading to a desired result. The steps are those requiring physical manipulations of data representing physical quantities to achieve tangible and useful results. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers or the like.

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussions, it is appreciated that throughout the present invention, discussions utilizing terms such as "receiving", "allowing", "processing", "interpreting", "providing" or the like, refer to the actions and processes of a computer system, or similar electronic computing device, such as intelligent hardware or an intelligent data concentrator. The computer system or similar electronic device manipulates and transforms data represented as electronic quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission, or display devices.

Portions of the present invention are comprised of computer-readable and computer executable instructions which reside, for example, in computer-usable media of a computer system or intelligent hardware (e.g., an intelligent data concentrator). It is appreciated that the present invention can operate within a number of different computer systems including general purpose computer systems, embedded computer systems, and stand alone computer systems specially adapted for controlling automatic test equipment.

The present invention provides a device and method for power management of electronic devices in a personal area network coupled to intelligent hardware, also referred to herein as an intelligent data concentrator. Specifically, the present invention also provides a method and a device thereof for automatically turning off the electronic devices or placing the electronic devices in a low power mode when they are not being used or according to predefined criteria. The described method can be controlled from a remote central control site communicatively coupled to the intelligent hardware over the network, or can be controlled directly from the intelligent hardware.

Figure 1 illustrates an exemplary personal area network (PAN) 100 coupled to a local area network (LAN) 150 in accordance with one embodiment of the present invention. PAN 100 comprises IP telephony 110, notebook 120, desktop workstation 130, and printer 140, each of which is communicatively coupled to intelligent data concentrator 210. Intelligent data concentrator 210 is coupled to LAN 150, thus acting as an interface from the various client devices (e.g., comprises IP telephony 110, notebook 120, desktop workstation 130, and printer 140) to LAN 150.

In one embodiment, the electronic devices of PAN 100 (e.g., comprises IP telephony 110, notebook 120, desktop workstation 130, and printer 140) receive power over LAN 150 through intelligent data concentrator 210. In the

present embodiment, a remote power source transmits power across LAN 150 to intelligent data concentrator 210. Electronic devices coupled to intelligent data concentrator 210 are configured to receive the power they require to operate over LAN 150.

Figure 2 is a block diagram 200 of a cross-sectional view of an intelligent data concentrator 210 in accordance with one embodiment of the present invention. This embodiment of the present invention implements intelligent hardware that is easy to install and reliably provides an attachment point for access to voice and data networks 240. The embodiment is implemented through miniaturized hardware that can be installed inside of a wall or in internal space provided for in an office cubicle. One surface 230 of this embodiment is intended to be accessible by the end user and would in most instances be on an external surface of a workspace.

A plurality of ports 220 are mounted on the external surface 230 of this embodiment. In one embodiment, communication port 220 is an RJ-45 jack. In another embodiment, port 220 is an RJ-11 jack. It should be appreciated that port 220 is not limited to any particular jack, and that any type of communication port can be used. Additionally, while intelligent data concentrator 210 illustrates four ports 220, it should be appreciated that alternative implementations could support a greater or lesser number of ports 220.

Connections to the central data (LAN) or voice network 240[5] are terminated at intelligent data concentrator 210[5] for coupling to ports 220.[5] Termination of the network cabling 250[5] (voice or data) will provide for both a reliable electrical and mechanical connection for industry standard communications cabling such as CAT-3, CAT-5, CAT-5E or similar cabling.

In one embodiment, intelligent data concentrator 210[5] receives power over network cabling 250[5] from network 240.[5] A remote power source 260[5] transmits power over network cabling 250[5] to provide intelligent data concentrator 210[5] with the power it requires to operate. In one embodiment, intelligent data concentrator 210[5] is configured to transmit power to connected electronic devices through ports 220.[5]

Figure 3[5] is an illustration of a perspective view 300[5] of an exemplary user-accessible surface 230[5] of an intelligent data concentrator 210[5] in accordance with one embodiment of the present invention. A user is able to connect data devices to a voice or data network through ports 220.[5] As described above, in one embodiment of the present invention, intelligent data concentrator 210[5] is configured to transmit power to connected electronic devices through ports 220.[5]

Figure 4 is a block diagram of an exemplary LAN 400 upon which embodiments of the present invention may be practiced. In one embodiment, LAN 400 comprises a central control site 405 and intelligent hardware 410, 415, and 420. In one embodiment, intelligent hardware 410, 415 and 420 are intelligent data concentrators (e.g., intelligent data concentrator 210 of Figure 2 or intelligent data concentrator 602 of Figure 6). In one embodiment, central control site 405 can access the intelligence (e.g., intelligence 612 of Figure 6) of intelligent hardware 410, 415 and 420. In another embodiment, central control site 405 is a central data switch or hub. Intelligent hardware 410, 415 and 420 are communicatively coupled to central control site 405 over links 440, 445 and 450, respectively. In one embodiment, links 440, 445 and 450 are network cabling. In one embodiment, links 440, 445 and 450 also are coupled a power source (e.g. power source 250 of Figure 2 or power source 609 of Figure 6), such that they provide power to intelligent hardware 410, 415 and 420.

In one embodiment, intelligent hardware 410, 415 and 420 are connected to central control site 405 by means of network cabling. In the current embodiment, CAT 3 or 5 cabling is used and an Ethernet physical interface is employed. However, it should be appreciated that the present invention will work with other types of LANs, such as LANs with differing physical connections or adopted for use in RF wireless and optical systems. As discussed above, in one embodiment, links 440, 445 and 450 also provide

power to intelligent hardware 410, 415 and 420. In one embodiment, the power is supplied over network cabling.

Intelligent hardware 410 is coupled to electronic devices 425a and 425b. Similarly, intelligent hardware 415 is coupled to electronic devices 430a, 430b and 430c, and intelligent hardware 420 is coupled to electronic devices 435a and 435b. It should be appreciated that electronic devices can comprise any number of data devices or client devices, including but not limited to: computer systems, printers, voice IP telephones, and fax machines configured for use over voice IP networks.

In one embodiment, the intelligent hardware is configured to provide power to connected electronic devices. For example, in the present embodiment, intelligent hardware 410 supplies power to electronic devices 425a and 425b. It should be appreciated that electronic devices connected to an intelligent hardware may receive power over LAN 400. Power is supplied to the intelligent hardware, and an electronic device configured to receive power through the intelligent hardware receives its operating power through the intelligent hardware.

Figure 5 is a flowchart diagram of the steps in a process 500 for power management of intelligent hardware (e.g., an intelligent data concentrator) for providing access to voice and data networks. Steps of process 500, in the

present embodiment, may be implemented with any computer languages used by those of ordinary skill in the art.

At step 510, power use data of the intelligent hardware (e.g., intelligent data concentrator 210 of Figure 2 or intelligent data concentrator 602 of Figure 6) is obtained. As described above, the intelligent hardware is coupled to a power source and communicatively coupled to a voice or data network. The intelligent hardware is configured to communicatively couple a plurality of electronic devices to the network.

At step 520, using the power use data, a power mode of the intelligent hardware is determined. In one embodiment, the power use data is defined at a central control site communicatively coupled over the network to the intelligent hardware. The central control site has stored upon it instructions regarding the power mode of all connected intelligent hardware. In one embodiment, the power use data is user-defined.

In another embodiment, the power use data is predefined and stored in intelligence of said intelligent hardware. In one embodiment, the power use data is user-defined, and programmed directly into the intelligent hardware. In one embodiment, the power use data is entered into the intelligent hardware by a coupled electronic device.

In one embodiment, the low power mode or off mode is activated according to a predetermined power use data based on the time of day, week, or year. For example, a low power mode will automatically be activated after working hours (e.g., 6:00 PM through 6:00 AM), over weekends, or during holidays.

It should be appreciated that the present invention is customizable to fit the needs of specific users. For example, if boot time for a device is short, the intelligent hardware can be powered down in the evenings. Conversely, if boot time is long, only specific parts of the intelligent hardware may be powered down. Thus, a user is provided with a low power mode without disrupting their specific power needs.

In one embodiment, the power use data is obtained by detecting a level of activity of said intelligent hardware. In the present embodiment, if the intelligent hardware does not detect a predetermined level of activity for a predetermined period of time, the intelligent hardware will automatically be placed in a low power mode or off mode. For example, if the intelligent hardware detects no data transfer for a period of one hour, the intelligent hardware will automatically be placed in a low power mode or off mode. In one embodiment, once a client device begins a data transfer, the intelligent hardware is powered on, such that a user is not required to actively power on the device.

In another embodiment, activity logs of the intelligent hardware's activities is kept. The intelligent hardware will implicitly customize its power management to power on the device in times of typical user interaction and power off the device in times of no user interaction. For example, if data transfer occurs over the intelligent hardware every weekday from 7:00 AM to 5:00 PM, the intelligent hardware will power on the device during those hours. During hours of typical non-use, the intelligent hardware will be powered off.

In one embodiment, if no activity is detected over a period of days, the intelligent hardware will automatically shut off completely. In the present embodiment, the intelligent hardware determines that the office or cubicle in which the intelligent hardware is located is empty, thus necessitating a full power off. In the present embodiment, the intelligent hardware will notify the central operating unit of the shutting off of the intelligent hardware due to empty office or cube space.

In one embodiment, the intelligent hardware comprises a sensor (e.g., sensor 620 of Figure 6). In one embodiment, the present invention comprises a motion sensor for detecting a level of motion in a predetermined area containing the electronic device. In another embodiment, the present invention comprises a heat sensor for detecting a level of heat within an area. In another

embodiment, the present invention comprises a sound detector (e.g., a microphone) for detecting level of sound within an area.

In one embodiment, upon the level of detected motion falling below a user-defined minimum threshold, the intelligent hardware automatically turns off or is placed in a low power mode. Upon the level of motion falling below a minimum threshold, the intelligent hardware infers that no one is in the room at which the intelligent hardware is located. Thus, no one is using the intelligent hardware and the intelligent hardware automatically shuts off or powered down.

In another embodiment, upon the level of detected heat falling below a user-defined minimum threshold, the intelligent hardware automatically turns off or is placed in a low power mode. Upon the level of heat falling below a minimum threshold, the intelligent hardware infers that no one is in the room at which the intelligent hardware is located. Thus, no one is using the intelligent hardware and the electronic device automatically shuts off or is powered down.

Similarly, In another embodiment, upon the level of detected sound falling below a user-defined minimum threshold, the intelligent hardware automatically turns off or is placed in a low power mode. Upon the level of sound falling below a minimum threshold, the intelligent hardware infers that no one is in the room at which the intelligent hardware is located. Thus, no one

is using the intelligent hardware and the intelligent hardware automatically shuts off or is powered down.

In another embodiment, upon any combination of the level of detected motion falling below a user-defined minimum threshold, the level of detected heat falling below a user-defined minimum threshold, and the level of detected sound falling below a user-defined minimum threshold, the intelligent hardware automatically turns off or is placed in a low power mode. The intelligent hardware infers that no one is in the room at which the electronic device is located. Thus, no one is using the intelligent hardware and the intelligent hardware automatically shuts off or is powered down.

In another embodiment, once the level of detected motion, level of detected heat, or level of detected sound falls below a user-defined threshold, a timer is activated. Upon the passing of a first predetermined time period, the intelligent hardware automatically turns off or is placed in a low power mode.

The present invention provides for a method and a device thereof for automatically turning off an intelligent hardware when it is not being used, therefore reducing power costs and wear on the components of the intelligent hardware.

It should be appreciated that a low power mode (e.g., data transfer detection is possible) and a power off mode (e.g., no data transfer detection is possible) are both available to the above embodiments. While some embodiments lend themselves to one mode over the other, it should be appreciated that either mode is available for all embodiments discussed above.

Figure 6 is a block diagram 600 of an intelligent data concentrator 602 configured for performing a process of selectively providing access to a network in accordance with an embodiment of the present invention.

Intelligent data concentrator 602 comprises a first interface 604 for communicatively coupling intelligent data concentrator 602 to network 608 and for receiving power transmitted from power source 609 over network 608. Intelligent data concentrator 602 also comprises a plurality of second interfaces 606a-d for communicatively coupling intelligent data concentrator 602 to a plurality of electronic devices 610a-d. In one embodiment, second interfaces 606a-d are communication ports (e.g., communication ports 220 of Figure 2). It should be appreciated that there can be any number of second interfaces 606a-d, and that the present invention is not meant to limit the number of second interfaces 606a-d. First interface 604 operating in conjunction with second interfaces 606a-d operates to connect electronic devices 610a-d to network 608.

In another embodiment, second interfaces 606a-d[5] are configured to provide power to connected electronic devices. In the present embodiment, first interface 604[5] operating in conjunction with second interfaces 606a-d[5] operates to connect electronic devices 610a-d[5] to power source 609[5], thus providing electronic devices 610a-d[5] with power.

Intelligent data concentrator 602[5] also comprises intelligence 612[5]. In one embodiment, intelligence 612[5] comprises means for processing and interpreting data 614[5] coupled to the first interface 604[5], power mode control means 616[5] coupled to the means for processing and interpreting data 614[5], and data storage means 618[5]. Means for processing and interpreting data 614[5] is intended to include, but not limited to: a processor, a robust processor and a central processing unit (CPU). Data storage means is intended to include, but not limited to: random access memory (RAM), read-only memory (ROM), and flash memory.

In one embodiment, power mode control means 616[5] is a software implementation (e.g., a hardware power mode controller) in intelligent data concentrator 602[5]. Alternatively, power mode control means 616[5] can be implemented by hardware or firmware (e.g., a software or firmware power mode controller). In one embodiment, power mode control means 616[5] is

operable to place intelligent data concentrator 602 in either a standard operating mode or a low power or power off mode.

In one embodiment, power mode control means 616 operates to detect a level of activity (e.g., data transfer) between first interface 604 and second interfaces 606a-d, and adjust the power mode of intelligent data concentrator 602 accordingly. In one embodiment, intelligent data concentrator 602 has instructions stored in data storage means 618 for operating power mode control means 616.

In one embodiment, power mode control means 616 operates in conjunction with a central control site (e.g., central control site 405 of Figure 4) of network 608 for performing power management. In another embodiment, power mode control means is controlled by a central control site (e.g., central control site 405 of Figure 4) for adjusting the power mode of intelligent data concentrator 602.

Intelligent data concentrator 602 also comprises a sensor 620 coupled to intelligence 612. In one embodiment, sensor 620 is a motion sensor for detecting a level of motion in a predetermined area containing intelligent data concentrator 602. In another embodiment, sensor 620 is a heat sensor for detecting a level of heat within an area. In another embodiment, sensor 620 is a sound detector (e.g., a microphone) for detecting a level of sound within an

area. The functionality of sensor 620 is described in detail above with reference to Figure 5.

The preferred embodiment of the present invention, a method for power management of intelligent hardware for providing access to voice and data networks, is thus described. While the present invention has been described in particular embodiments, it should be appreciated that the present invention should not be construed as limited by such embodiments, but rather construed according to the below claims.

SECTION 6

A secure network outlet for supporting IP device address assigning functionality. A network access request is received from an electronic device communicatively coupled to intelligent hardware. In one embodiment, a device address request is transmitted to a network server. A first device address is received at the intelligent hardware from the network server. The intelligent hardware then assigns a second device address to the electronic device. In another embodiment, the intelligent hardware has a pre-assigned first device address and assigns a second device address to the electronic device, such that the intelligent hardware eliminates the need for a separate device address assigning server. The present invention reduces the consumption of global device addresses within a network, and also provides protection to electronic devices by hiding their device addresses from the external network.

SECTION 6

This section 6 relates to the field of computer networks. In particular, this section 6 relates to a secure network outlet for supporting internet protocol (IP) device address assigning functionality in an intelligent data concentrator.

BACKGROUND

As computer networks increasingly proliferate in society, the number of devices coupled to computer networks grows at a fast rate. Traditionally, one cable connects a single RJ-45 port of the outlet to a local area network (LAN) wiring closet and multiple ports requires additional wiring. A network outlet, such as a switch or a hub, connects multiple network devices to LAN port located in a wiring closet.

Additional cables are needed for multiple ports on the network outlet, thereby increasing the network layout and cabling while limiting network accessibility. As one cable is required to connect each computer to the LAN port of the wiring closet, the costs associated with connecting more computers to the LAN are very high, particularly in wiring and installation costs. Additionally, each computer requires a unique global IP address assigned to the outlet. As such, a large number of global IP addresses are consumed.

One limitation with regards to computer networks is that there are only a limited number of global IP addresses. As it is becoming more necessary to connect more computers to LANs and the Internet, the number of global IP addresses being consumed is increasing, thus decreasing the available number of global IP addresses. Implementing Network Address Translation (NAT) technology in a network outlet is useful in saving the consumption of the global routable IP addresses within a LAN. Under NAT, one global IP address is assigned to the outlet for connection to the LAN while private IP addresses are used to control multiple devices within the personal area network (PAN).

One drawback to the use of network outlets, such as a stand-alone switch or a firewall device, is that the are subject to misuse or theft. Network outlets are typically unmanaged and do not have built-in access control. In particular, network outlets are typically not secure. Furthermore, network outlets implementing firewall/security policies are not centrally managed or distributed by a trusted source.

Accordingly, a need exists for a secure network outlet for coupling an electronic device to a network. A need also exists for a method and a device thereof which satisfies the above need for supporting IP device address assigning functionality. A need also exists for a method and device thereof which satisfies the above needs and which reduces the consumption of available global IP addresses within a network. A need also exists for a

method and device thereof that satisfies the above needs and also protects PAN devices by hiding their IP addresses from the external network.

SUMMARY

The present invention provides a secure network outlet for coupling an electronic device to a network. The present invention also provides a method and a device for supporting IP device address assigning functionality. The present invention also provides a method and device that reduces the consumption of available global IP addresses within a network. The present invention also provides a method and device that protects PAN devices by hiding their IP addresses from the external network.

In one embodiment, the present invention provides a method for performing device address assigning functionality in intelligent hardware. A network access request is received from an electronic device communicatively coupled to the intelligent hardware. In one embodiment, a device address request is transmitted to a network server. A first device address is received at the intelligent hardware from the network server. The intelligent hardware then assigns a second device address to the electronic device.

In another embodiment, the intelligent hardware has a pre-assigned first device address and assigns a second device address to the electronic device, such that the intelligent hardware eliminates the need for a separate device address assigning server. The present invention reduces the consumption of global device addresses within a network, and also provides protection to electronic devices by hiding their device addresses from the external network.

In one embodiment, the present invention comprises a first interface for communicatively coupling the intelligent hardware to the network and a second interface for communicatively coupling the intelligent device to a plurality of client devices. The intelligent device also comprises a processor coupled to the first interface. In one embodiment, the intelligent device also comprises a device address retriever for retrieving a device address from a network server and assigning a device address to a connected electronic device. In another embodiment, the intelligent device also comprises a device address assignor for assigning a device address to a connected electronic device, such that the intelligent device eliminates the need for a separate device address assigning server (e.g., network server).

These and other objects and advantages of the present invention will become obvious to those of ordinary skill in the art after having read the following detailed description of the preferred embodiments which are illustrated in the various drawing figures.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and form a part of this specification, illustrate embodiments of the invention and, together with the description, serve to explain the principles of the invention:

FIGURE 1 illustrates an exemplary wired desktop cluster coupled to a local area network (LAN) in accordance with one embodiment of the present invention.

FIGURE 2 is a block diagram of a cross-sectional view of an intelligent data concentrator in accordance with one embodiment of the present invention.

FIGURE 3 is an illustration of a perspective view of an exemplary faceplate of an intelligent data concentrator in accordance with one embodiment of the present invention.

FIGURE 4 is a block diagram of an exemplary network upon which embodiments of the present invention may be practiced.

FIGURE 5 is a flowchart diagram of the steps in a process for performing device address assigning functionality in intelligent hardware (e.g.,

an intelligent data concentrator) having a device address retriever in accordance with one embodiment of the present invention.

FIGURE 6 is a flowchart diagram of the steps in a process for performing device address assigning functionality in intelligent hardware (e.g., an intelligent data concentrator) having a device address assignor in accordance with one embodiment of the present invention.

FIGURE 7 is a block diagram of an intelligent data concentrator having a device address retriever configured for performing device address assigning functionality in accordance with an embodiment of the present invention.

FIGURE 8 is a block diagram of an intelligent data concentrator having a device address assignor configured for performing device address assigning functionality in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION

In the following detailed description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that the present invention may be practiced without these specific details. In other instances, well-known structures and devices are not described in detail in order to avoid obscuring aspects of the present invention.

Some portions of the detailed descriptions which follow are presented in terms of procedures, steps, logic blocks, processing, and other symbolic representations of operations on data bits within a computer memory. These descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. A procedure, computer executed step, logic block, process, etc., is here and generally conceived to be a self-consistent sequence of steps of instructions leading to a desired result. The steps are those requiring physical manipulations of data representing physical quantities to achieve tangible and useful results. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers or the like.

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussions, it is appreciated that throughout the present invention, discussions utilizing terms such as "receiving", "transmitting", "assigning", "performing", "providing" or the like, refer to the actions and processes of a computer system, or similar electronic computing device, such as intelligent hardware or an intelligent data concentrator. The computer system or similar electronic device manipulates and transforms data represented as electronic quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission, or display devices.

Portions of the present invention are comprised of computer-readable and computer executable instructions which reside, for example, in computer-usable media of a computer system or intelligent hardware (e.g., an intelligent data concentrator). It is appreciated that the present invention can operate within a number of different computer systems including general purpose computer systems, embedded computer systems, and stand alone computer systems specially adapted for controlling automatic test equipment.

The present invention provides a secure network outlet for supporting IP device address assigning functionality. Specifically, the present invention provides intelligent hardware (e.g., an intelligent data concentrator) for assigning a device address to an electronic device communicatively coupled to the intelligent hardware. In one embodiment, the intelligent hardware can operate as either a device address retriever for communicating with a network server for assigning a device address. In another embodiment, the intelligent hardware operates as a network server for assigning a device address, such that the intelligent hardware eliminates the need for a separate device address assigning server.

Figure 1 illustrates an exemplary personal area network (PAN) 100 coupled to a local area network (LAN) 150 in accordance with one embodiment of the present invention. PAN 100 comprises IP telephony 110, notebook 120, desktop workstation 130, and printer 140, each of which is communicatively coupled to intelligent data concentrator 210. Intelligent data concentrator 210 is coupled to LAN 150, thus acting as an interface from the various client devices (e.g., comprises IP telephony 110, notebook 120, desktop workstation 130, and printer 140) to LAN 150.

In one embodiment, the electronic devices of PAN 100 (e.g., comprises IP telephony 110, notebook 120, desktop workstation 130, and printer 140)

receive power over LAN 150 through intelligent data concentrator 210. In the present embodiment, a remote power source transmits power across LAN 150 to intelligent data concentrator 210. Electronic devices coupled to intelligent data concentrator 210 may be configured to receive power over LAN 150.

Figure 2 is a block diagram 200 of a cross-sectional view of an intelligent data concentrator 210 in accordance with one embodiment of the present invention. This embodiment of the present invention implements intelligent hardware that is easy to install and reliably provides an attachment point for access to voice and data networks 240. The embodiment is implemented through miniaturized hardware that can be installed inside of a wall or in internal space provided for in an office cubicle. One surface 230 of this embodiment is intended to be accessible by the end user and would in most instances be on an external surface of a workspace.

A plurality of ports 220 are mounted on the external surface 230 of this embodiment. In one embodiment, communication port 220 is an RJ-45 jack. In another embodiment, port 220 is an RJ-11 jack. It should be appreciated that port 220 is not limited to any particular jack, and that any type of communication port can be used. Additionally, while intelligent data concentrator 210 illustrates four ports 220, it should be appreciated that alternative implementations could support a greater or lesser number of ports 220.

Connections to the central data (LAN) or voice network 240 are terminated at intelligent data concentrator 210 for coupling to ports 220. Termination of the network cabling 250 (voice or data) will provide for both a reliable electrical and mechanical connection for industry standard communications cabling such as CAT-3, CAT-5, CAT-5E or similar cabling.

In one embodiment, intelligent data concentrator 210 assigns a device address to electronic devices connected through ports 220 for communicating over network 240. Intelligent data concentrator 240 communicates with remote network server 260 for assigning device addresses to connected electronic devices. In one embodiment, intelligent data concentrator 210 operates as a device address retriever for communicating with network server 260 for assigning a device address.

In one embodiment, mounting hardware attaching intelligent data concentrator 210 to the wall also comprises a tamper detection means 270. In one embodiment, tamper detection means 270 is tamper detection hardware or a tamper detection switch. If a user attempts to circumvent the security measures by physically removing intelligent data concentrator 210, the act of removing the mounting screws would be detected by tamper detection means 270 and an alerting message would be transmitted to a central control site over network 240. In one embodiment, the attempt would be logged and a control

message could be sent to a centralized management station that could disallow network traffic on the segment that intelligent data concentrator 210 was attached to.

Figure 3 is an illustration of a perspective view 300 of an exemplary user-accessible surface 230 of an intelligent data concentrator 210 in accordance with one embodiment of the present invention. A user is able to connect data devices to a voice or data network through ports 220. As described above, in one embodiment of the present invention, intelligent data concentrator 210 is configured to transmit power to connected electronic devices through ports 220.

Figure 4 is a block diagram of an exemplary LAN 400 upon which embodiments of the present invention may be practiced. In one embodiment, LAN 400 comprises network server 405 and intelligent hardware 410, 415, and 420. In one embodiment, intelligent hardware 410, 415 and 420 are intelligent data concentrators (e.g., intelligent data concentrator 210 of Figure 2, intelligent data concentrator 702 of Figure 7 or intelligent data concentrator 802 of Figure 8). In one embodiment, network server 405 is used for retrieving and assigning a device address to an electronic device communicatively coupled to intelligent hardware 410, 415 and 420. 420 are communicatively coupled to network server 405 over links 440, 445 and 450, respectively. In one embodiment, links 440, 445 and 450 are network cabling. In one embodiment,

links 440, 445 and 450 also are coupled a power source (e.g. power source 250 of Figure 2 or power source 609 of Figure 6), such that they provide power to intelligent hardware 410, 415 and 420.

In one embodiment, intelligent hardware 410, 415 and 420 are connected to network server 405 by means of network cabling. In the current embodiment, CAT 3 or 5 cabling is used and an Ethernet physical interface is employed. However, it should be appreciated that the present invention will work with other types of LANs, such as LANs with differing physical connections or adopted for use in RF wireless and optical systems. As discussed above, In one embodiment, links 440, 445 and 450 also provide power to intelligent hardware 410, 415 and 420. In one embodiment, the power is supplied over network cabling.

Intelligent hardware 410 is coupled to electronic devices 425a and 425b. Similarly, intelligent hardware 415 is coupled to electronic devices 430a, 430b and 430c, and intelligent hardware 420 is coupled to electronic devices 435a and 435b. It should be appreciated that electronic devices can comprise any number of data devices or client devices, including but not limited to: computer systems, printers, voice IP telephones, and fax machines configured for use over voice IP networks.

In one embodiment, the intelligent hardware is configured to provide power to connected electronic devices. For example, in the present embodiment, intelligent hardware 410 supplies power to electronic devices 425a and 425b. It should be appreciated that electronic devices connected to an intelligent hardware may receive power over LAN 400. Power is supplied to the intelligent hardware, and an electronic device configured to receive power through the intelligent hardware receives its operating power through the intelligent hardware.

Figure 5 is a flowchart diagram of the steps in a process 500 for performing device address assigning functionality in intelligent hardware (e.g., intelligent data concentrator 702 of Figure 7) having a device address retriever in accordance with one embodiment of the present invention. Steps of process 500, in the present embodiment, may be implemented with any computer languages used by those of ordinary skill in the art.

At step 510 of process 500, the intelligent hardware having a device address retriever receives a network access request from a connected electronic device. It should be appreciated that a network access request is intended to include any request for data over a network. In one embodiment, the network access request is a request to communicate with a computer system located on a corporate network. In another embodiment, the network

access request is a request to communicate with a computer system located on the Internet.

At step 520, the intelligent hardware transmits a device address request to a network server. It should be appreciated that in order for an electronic device to communicate over a network, it requires a device address. The device address operates to ensure that data packets are sent to the correct electronic device. In one embodiment, the device address is an Internet Protocol (IP) address. In one embodiment, the network server is a Dynamic Host Configuration Protocol (DHCP) server.

At step 530, the intelligent hardware receives a device address (e.g., and IP address) from the network server. In one embodiment, the device address is a global IP address.

At step 540, the intelligent hardware assigns a device address to the electronic device. In one embodiment, the intelligent hardware assigns the device address received from the network server to the electronic device. In another embodiment, the intelligent hardware assigns the electronic device a private device address. In one embodiment, the private device address is a private IP address. The present embodiment protects electronic devices connected to the intelligent hardware by hiding their IP addresses from the external network.

Figure 6 is a flowchart diagram of the steps in a process 600 for performing device address assigning functionality in intelligent hardware (e.g., intelligent data concentrator 802 of Figure 8) having a device address assignor in accordance with one embodiment of the present invention. Steps of process 600, in the present embodiment, may be implemented with any computer languages used by those of ordinary skill in the art.

At step 610 of process 600, the intelligent hardware having a device address assignor receives a network access request from a connected electronic device. It should be appreciated that a network access request is intended to include any request for data over a network. In one embodiment, the network access request is a request to communicate with a computer system located on a corporate network. In another embodiment, the network access request is a request to communicate with a computer system located on the Internet.

At step 620, the intelligent hardware assigns a device address to the electronic device, such that said intelligent hardware eliminates the need for a separate device address assigning server. In the present embodiment, the device address assignor operates as a device address assigning server. In one embodiment, the device address assignor operates as a DHCP server.

In one embodiment, the intelligent hardware assigns the electronic device a public device address. In another embodiment, the intelligent hardware assigns the electronic device a private device address. In one embodiment, the private device address is a private IP address. The present embodiment protects electronic devices connected to the intelligent hardware by hiding their IP addresses from the external network. In one embodiment, the intelligent hardware has a preassigned device address.

Figure 7 is a block diagram 700 of an intelligent data concentrator 702 having a device address retriever 716 configured for performing device address assigning functionality in accordance with an embodiment of the present invention. In one embodiment, intelligent data concentrator 702 is configured to perform a process for performing device address assigning functionality as described above in process 500 of Figure 5.

Intelligent data concentrator 702 comprises a first interface 704 for communicatively coupling intelligent data concentrator 702 to network 708. Intelligent data concentrator 702 also comprises a plurality of second interfaces 706a-d for communicatively coupling intelligent data concentrator 702 to a plurality of electronic devices 710a-d. In one embodiment, second interfaces 706a-d are communication ports (e.g., communication ports 220 of Figure 2). It should be appreciated that there can be any number of second interfaces 706a-d, and that the present invention is not meant to limit the

number of second interfaces 706a-d. First interface 704 operating in conjunction with second interfaces 706a-d operates to connect electronic devices 710a-d to network 708.

Intelligent data concentrator 702 also comprises intelligence 712. In one embodiment, intelligence 712 comprises processor 714 coupled to the first interface 704 and status device address retriever 716 coupled to the means for processing and interpreting data 714. In one embodiment, processor 714 is a robust processor. In another embodiment, processor 714 is a central processing unit (CPU).

In one embodiment, device address retriever 716 is a software implementation in intelligent data concentrator 702. Alternatively, device address retriever 716 can be implemented by hardware or firmware (e.g., a software or firmware device address retriever).

In one embodiment, device address retriever 716 operates to obtain a device address for electronic devices connected to intelligent data concentrator 702 through second interfaces 706a-d by communicating with network server 709. In one embodiment, network server 709 is a DHCP server. In one embodiment, the device addresses are IP addresses.

Figure 8 is a block diagram 800 of an intelligent data concentrator 802 having a device address assignor 816 configured for performing device address assigning functionality in accordance with an embodiment of the present invention. In one embodiment, intelligent data concentrator 802 is configured to perform a process for performing device address assigning functionality as described above in process 600 of Figure 6.

Intelligent data concentrator 802 comprises a first interface 804 for communicatively coupling intelligent data concentrator 802 to network 808. Intelligent data concentrator 802 also comprises a plurality of second interfaces 806a-d for communicatively coupling intelligent data concentrator 802 to a plurality of electronic devices 810a-d. In one embodiment, second interfaces 806a-d are communication ports (e.g., communication ports 220 of Figure 2). It should be appreciated that there can be any number of second interfaces 806a-d, and that the present invention is not meant to limit the number of second interfaces 806a-d. First interface 804 operating in conjunction with second interfaces 806a-d operates to connect electronic devices 810a-d to network 808.

Intelligent data concentrator 802 also comprises intelligence 812. In one embodiment, intelligence 812 comprises processor 814 coupled to the first interface 804 and device address assignor 816 coupled to the means for processing and interpreting data 814. In one embodiment, processor 814 is a

robust processor. In another embodiment, processor 814 is a central processing unit (CPU).

In one embodiment, device address assignor 816 is a software implementation in intelligent data concentrator 802. Alternatively, device address assignor 816 can be implemented by hardware or firmware (e.g., a software or firmware device address assignor). In one embodiment, device address assignor 816 is a DHCP server.

In one embodiment, device address assignor 816 operates to assign a device address for electronic devices connected to intelligent data concentrator 802 through second interfaces 806a-d without requiring a separate device assigning server. In one embodiment, the device addresses are IP addresses. In one embodiment, intelligent data concentrator 802 has a pre-assigned device address.

The preferred embodiment of the present invention, a secure network outlet for supporting IP device address assigning functionality, is thus described. While the present invention has been described in particular embodiments, it should be appreciated that the present invention should not be construed as limited by such embodiments, but rather construed according to the below claims.

CLAIMS

We claim:

1. A method for managing wireless access to a network, comprising:

providing wireless communication in a network;

providing a firewall protection between said network and a wireless access device;

submitting an identification code to said network from said wireless access device;

determining the validity of said identification code;

granting wireless network access to said wireless access device when said identification code is valid;

denying wireless network access to said wireless access device when said identification code is not valid; and

issuing an alert when said identification code is not valid.

2. The method described in Claim 1, wherein said providing said wireless communication is accomplished with an intelligent concentrator enabled for wireless communication.

3. The method described in Claim 2, wherein said providing said wireless communication is accomplished in circuitry resident in said intelligent concentrator.

4. The method described in Claim 1, wherein said identification code is the media access control number of said wireless access device.

5. The method described in Claim 1, wherein said determining said validity of said identification code is accomplished by reference to a list of valid identification codes.

6. The method described in Claim 5, wherein said list of valid identification codes is resident in said intelligent

concentrator.

7. The method described in Claim 5, wherein said list of valid identification codes is resident in a server in said network.

8. The method described in Claim 1, wherein said denying said wireless access to said network is accomplished simultaneously with granting access to wireless access devices with valid identification codes.

9. The method described in Claim 1, wherein said network is a wireless personal area network.

10. A computer network, comprising:

a server;

a wireless connection device communicatively coupled with said server;

a wireless access device enabled to wirelessly submit an identification code to said wireless connection device; and

a firewall communicatively coupled to said server and said wireless connection device, wherein said firewall is enable to grant network access to said wireless access device when said identification code is valid and to deny access to said network by said wireless access device and issue an alert when said identification code is not valid.

11. The computer network described in Claim 10, wherein said server is an internet portal.

12. The computer network described in Claim 10, wherein said wireless connection device is an intelligent concentrator enabled for wireless communication.

13. The computer network described in Claim 10, wherein said wireless access device is a wirelessly enabled laptop computer.

14. The computer network described in Claim 10, wherein said

wireless access device is a wirelessly enabled personal data assistant.

15. The computer network described in Claim 10, wherein said wireless access device is a wireless telephone enabled for data communication.

16. The computer network described in Claim 10, wherein said wireless access device is a wirelessly enabled computer peripheral device.

17. The computer network described in Claim 10, wherein said firewall is a distributed firewall and is resident in said intelligent concentrator.

18. The computer network described in Claim 17, wherein said distributed firewall is enabled to obtain a list of valid identification codes from said server.

19. The network described in Claim 18, wherein said distributed firewall is enabled to verify the validity of said identification code submitted from a wireless access device.

20. An intelligent concentrator, comprising:

a housing;

a cable connector coupled to said housing and adapted to communicatively couple said intelligent concentrator to a network data cable;

electronic circuitry mounted in said housing enabled to wirelessly communicate with a wireless access device and a network; and

a distributed firewall resident in said electronic circuitry wherein said firewall is enabled to control the access to said network of said wireless access device.

21. The intelligent concentrator described in Claim 20, wherein said intelligent concentrator is enabled as a hub of a personal

area network.

22. The intelligent concentrator described in Claim 20, wherein said distributed firewall is enabled to obtain a list of valid identification codes from a server in said network.

23. The intelligent concentrator described in Claim 20, wherein said distributed firewall is enabled to verify validity of an identification code submitted by a wireless access device.

24. The intelligent concentrator described in Claim 20, wherein said distributed firewall is enabled to deny access to said wireless access device if said identification code is not valid.

25. The intelligent concentrator described in Claim 20, wherein said distributed firewall is enabled to issue an alarm to a network manager if said identification code is not valid.

26. A method for efficiently managing a network comprising:

a) providing an intelligent device, said intelligent device comprising:

a first interface for communicatively coupling said intelligent device to said network;

a second interface for communicatively coupling said intelligent device to a plurality of electronic devices such that each said electronic device is communicatively coupled to said network;

a processor coupled to said first interface and said second interface;and

a status information provider coupled to said processor; and

b) accessing said status information provider over said network such that said intelligent device is configured to be monitored remotely.

27. A method as recited in Claim 26 wherein said intelligent device is communicatively coupled over said network to a

computer system, said computer system for accessing said status information provider.

28. A method as recited in Claim 27 wherein said computer system is a remote monitoring unit.

29. A method as recited in Claim 26 wherein said status information provider is configured to obtain status information of said intelligent device and provide said status information of said intelligent device for remote access.

30. A method as recited in Claim 26 wherein said intelligent device is configured to be assigned a distinct device location identifier associated therewith.

31. A method as recited in Claim 26 wherein said electronic device is a client device.

32. A method as recited in Claim 27 wherein said computer system comprises a display for displaying said status information of said intelligent device.

33. A method as recited in Claim 32 wherein said display comprises a graphical user interface configured for allowing a user to interact with said status information of said intelligent device.

34. A method as recited in Claim 26 wherein a log is generated for said intelligent device, said for storing said status information therein.

35. A method as recited in Claim 32 wherein said display is for displaying graphical representation of said network.

36. A method as recited in Claim 26 wherein said intelligent device is coupled to a power source over said network, said power source for providing power to said intelligent device.

37. A method as recited in Claim 36 wherein a power level of said intelligent device is controlled over said network.

38. An intelligent device comprising:

a first interface for communicatively coupling said intelligent device to a network;

a second interface for communicatively coupling said intelligent device to a plurality of electronic devices such that each said electronic device is communicatively coupled to said network;

a processor coupled to said first interface and said second interface; and

a status information provider coupled to said processor, said status information provider configured to obtain status information of said intelligent device and provide said status information of said intelligent device for remote access.

39. The device of Claim 38 wherein the processor both processes and interprets data.

40. An intelligent device as recited in Claim 38 wherein said intelligent device is communicatively coupled over said network to a computer system, said computer system for accessing said status information provider.

41. An intelligent device as recited in Claim 40 wherein said computer system is a remote monitoring unit.

42. An intelligent device as recited in Claim 38 wherein said intelligent device is configured for assigning a distinct device location identifier associated therewith.

43. An intelligent device as recited in Claim 38 wherein said electronic device is a client device.

44. An intelligent device as recited in Claim 39 wherein said

computer system comprises a display for displaying said status information of said intelligent device.

45. An intelligent device as recited in Claim 42 wherein said display comprises a graphical user interface configured for allowing a user to interact with said status information of said intelligent device.

46. An intelligent device as recited in Claim 38 wherein a log is generated for said intelligent device, said for storing said status information therein.

47. An intelligent device as recited in Claim 44 wherein said display is for displaying graphical representation of said network.

48. An intelligent device as recited in Claim 38 wherein said intelligent device is coupled to a power source over said network, said power source for providing power to said intelligent device.

49. An intelligent device as recited in Claim 48 wherein a power level of said intelligent device is controlled over said network.

50. A multi-configuration network connection point device comprising:

a first connection interface including a primary connection port for communicatively coupling to an upstream network device;

a second connection interface including a secondary connection port for communicatively coupling to a downstream network device via a wireless technology, wherein said second connection interface is adapted to be secured in a fixed location while conveniently providing said communicatively coupling to a downstream network device via a wireless technology; and

a communication bus for communicatively coupling said first

connection interface to said second connection interface.

51. The device of Claim 50 wherein said interface is coupled to said body.

52. The device of Claim 50 further comprising:

a means for intelligently concentrating data from a plurality of interface connection ports included in said second connection interface for communication on said primary connection port of said first connection interface.

53. A multi-configuration network connection point device of Claim 50, 51, or 52 wherein said first connection interface comprises a single primary interface connection port.

54. A multi-configuration network connection point device of Claim 50, 51, or 52 wherein said secondary connection interface comprises a plurality of interface connection ports.

55. A multi-configuration network connection point device of Claim 50, 51, or 52 wherein said first connection interface couples to a singular communication path to an upstream device.

56. A multi-configuration network connection point device of Claim 50, 51, or 52 wherein said secondary connection interface is configured for convenient placement in fixed locations in a manner that facilitates maintenance of system integrity and security.

57. A multi-configuration network connection point device of Claim 52 further comprising a means for processing and interpreting data coupled to a first interface.

58. A multi-configuration network connection point device of Claim 57 further comprising a fault detection means coupled to the means for processing and interpreting data.

59. A multi-configuration network connection point device of Claim 52 further comprising:

a processing unit for processing information; and

a memory for storing said information.

60. A multi-configuration network connection point method comprising:

providing a single connection point on a primary communication interface;

providing a plurality of connection points on a secondary communication interface; and

coupling the single connection point on a primary communication interface to the plurality of connection points on a secondary communication interface.

61. The multi-configuration network connection point method of Claim 60 wherein the single connection point couples to a single communication path (e.g., to upstream network devices).

62. The multi-configuration network connection point method of Claim 60 wherein the single connection point is configured for fixed placement in a concealed environment.

63. The multi-configuration network connection point method of Claim 60 wherein the secondary communication interface is adapted to be secured in a fixed location while conveniently providing said communicatively coupling to a downstream network device via a wireless technology.

64. The multi-configuration network connection point method of Claim 60 further comprising intelligently concentrating data from a plurality of interface connection ports included of said second connection interface for communication on said primary connection port of a first connection interface.

65. An apparatus for multiplexing signals at a work center in a network, comprising:

a work center mountable housing;

two or more network connection devices coupled with said work center mountable housing;

cabling, electronically and communicatively coupling said apparatus with said network and enabled to carry said multiplexed signals;

an electrical power connection device; and,

electronic circuitry, coupled with said work center mountable housing and electrically and communicatively coupled with said network connection devices; wherein said electronic circuitry is enabled to control the multiplexing of said signals in network cabling connected to said network connection devices, such that multiplexing of signals emanating from said work center and demultiplexing of network signals intended for said work center are accomplished locally at said work center.

66. An apparatus as described in Claim 65 wherein said network connection devices are capable of connecting data lines.

67. An apparatus as described in Claim 65 wherein said network connection devices are capable of connecting voice telephone lines.

68. An apparatus as described in Claim 65 wherein said network connection devices are capable of connecting to and delivering device power.

69. An apparatus as described in Claim 65 wherein said electronic circuitry is capable of communicating system information to said network.

70. An apparatus as described in Claim 65 wherein said electronic circuitry is further enabled to assist maintenance of network security.

71. An apparatus as described in Claim 65 wherein said electronic circuitry is further enabled to assist monitoring of

device electrical power.

72. An apparatus as described in Claim 71 wherein said electronic circuitry is powered by said device electrical power.

73. A method for providing network device connection at a work center, comprising:

providing a network connection device at said work center capable of connecting a network device to a network;

sensing an identity of said network device when said network device is connected to said network connection device;

determining a power requirement of said network device;

delivering electrical power to said network device;

multiplexing data signals and said electrical power between said network and said network device; and

monitoring said electrical power supplied to said network device in said network.

74. The method described in Claim 73, wherein said step of providing a network connection device is accomplished with a modular cable connector.

75. The method described in Claim 73, wherein said step of multiplexing signals is capable of multiplexing network data signals.

76. The method described in Claim 73, wherein said step of multiplexing signals is capable of multiplexing voice telephone signals.

77. The method described in Claim 73, wherein said step of multiplexing signals is accomplished at said work center.

78. The method described in Claim 73, wherein said network connection device is enabled to connect to and deliver device electrical power.

79. The method described in Claim 73, wherein said network connection device is enabled to communicate system information to said network.

80. The method described in Claim 73, wherein said network connection device is enabled to monitor and control device power delivery.

81. A system for connecting a network, comprising:

a network comprising one or more servers and one or more work centers;

cabling communicatively connecting said work centers and said servers in said network;

cabling capable of delivering electrical power to said work centers; and,

one or more network connection devices enabled to intelligently multiplex communication and electrical power between a plurality of devices in said work centers and said network.

82. The system described in Claim 81, wherein said work centers comprise computers.

83. The system described in Claim 81, wherein said work centers comprise computer peripheral devices.

84. The system described in Claim 81, wherein said work centers comprise VOIP enabled telephones.

85. The system described in Claim 81, wherein said network connection devices are enabled to connect to other network connection devices in a daisy-chain fashion.

86. The system described in Claim 81, wherein said network connection devices comprise circuitry enabled to assist in maintaining the security of said network.

87. The system described in Claim 81, wherein said network connection devices comprise circuitry enabled to assist in managing the infrastructure of said network.

88. The system described in Claim 81, wherein said network connection devices comprise circuitry powered by said network device electrical power.

89. A method for controlling power for intelligent hardware comprising:
a) obtaining power use data of said intelligent hardware, said intelligent hardware coupled to a power source and communicatively coupled to a network and configured to communicatively couple a plurality of electronic devices to said network;
b) using said power use data to determine a power mode of said intelligent hardware.

90. A method as recited in Claim 89 wherein said intelligent hardware comprises:

a first interface for coupling said intelligent hardware to said power source and communicatively coupling said intelligent hardware to said network;

a second interface for communicatively coupling said intelligent hardware to said plurality of electronic devices such that each said electronic device is communicatively coupled to said network;

a processor coupled to said first interface and said second interface; and

a power mode controller coupled to said processor.

91. A method as recited in Claim 89 wherein said intelligent hardware is communicatively coupled over said network to a central control site, said central control site for defining said power use data.

92. A method as recited in Claim 89 wherein said power use data

is predefined and stored in intelligence of said intelligent hardware.

93. A method as recited in Claim 89 wherein said power use data is user-defined.

94. A method as recited in Claim 89 wherein said power use data is obtained by detecting a level of activity of said intelligent hardware.

95. A method as recited in Claim 89 wherein said power use data is obtained by detecting a level of activity within a predetermined area, said predetermined area containing said intelligent hardware.

96. A method as recited in Claim 95 wherein said level of activity is detected by a motion detector.

97. A method as recited in Claim 95 wherein said level of activity is detected by a heat sensor.

98. A method as recited in Claim 95 wherein said level of activity is detected by a sound detector.

99. A method as recited in Claim 89 wherein said intelligent hardware is configured to supply power from said power source to said plurality of electronic devices.

100. An intelligent device comprising:

a first interface for coupling said intelligent device to said power source and communicatively coupling said intelligent device to said network;

a second interface for communicatively coupling said intelligent device to a plurality of electronic devices such that each said electronic device is communicatively coupled to said network;

a processor coupled to said first interface and said second

interface; and

a power mode controller coupled to said processor, said power mode controller configured to obtain power use data of said intelligent device and configured to use said power use data to determine a power mode of said intelligent device.

101. The device of Claim 100 wherein said processor both processes and interprets data.

102. An intelligent device as recited in Claim 100 wherein said intelligent device is communicatively coupled over said network to a central control site, said central control site for defining said power use data.

103. An intelligent device as recited in Claim 100 wherein said power use data is predefined and stored in intelligence of said intelligent device.

104. An intelligent device as recited in Claim 100 wherein said power use data is user-defined.

105. An intelligent device as recited in Claim 100 wherein said power use data is obtained by detecting a level of activity of said intelligent device.

106. An intelligent device as recited in Claim 100 wherein said power use data is obtained by detecting a level of activity within a predetermined area, said predetermined area containing said intelligent device.

107. An intelligent device as recited in Claim 106 wherein said level of activity is detected by a motion detector.

108. An intelligent device as recited in Claim 106 wherein said level of activity is detected by a heat sensor.

109. An intelligent device as recited in Claim 106 wherein said

level of activity is detected by a sound detector.

110. An intelligent device as recited in Claim 101 wherein said intelligent device is configured to supply power from said power source to said electronic devices.

111. A method for performing device address assigning functionality in intelligent hardware, said method comprising:

receiving a network access request from an electronic device communicatively coupled to said intelligent hardware; and

assigning a device address to said electronic device communicatively coupled to said intelligent hardware.

112. The method of Claim 111 further comprising the steps of transmitting a device address request to a network server communicatively coupled to said intelligent hardware; receiving a first device address from said network server communicatively coupled to said intelligent hardware, the device address assigned to said electronic device communicatively coupled being a second device address.

113. The method of Claim 111 wherein said intelligent hardware having a first device address, said intelligent hardware eliminating the need for a separate device address assigning server, said assigning step assigning a second device address to said electronic device.

114. A method as recited in Claim 111, 112 or 113, wherein said intelligent hardware comprises:

a first interface for communicatively coupling said intelligent hardware to a network, said network comprising said network server;

a second interface for communicatively coupling said intelligent hardware to a plurality of said electronic devices such that each said electronic device is communicatively coupled to said network;

a processor coupled to said first interface and said second

interface; and

a device address retriever coupled to said processor.

115. A method as recited in Claim 112 or 113 wherein said first device address and said second device address are an IP addresses.

116. A method as recited in Claim 112 or 113 wherein said network server comprises a DHCP server.

117. A method as recited in Claim 112 or 113 wherein said first device address is the same as said second device address.

118. A method as recited in Claim 112 or 113 wherein said first device address is a global device address.

119. A method as recited in Claim 112 or 113 wherein said second device address is a private device address.

120. An intelligent device for performing device address assigning functionality comprising:

a first interface for communicatively coupling said intelligent device to a network;

a second interface for communicatively coupling said intelligent device to a plurality of electronic devices such that each said electronic device is communicatively coupled to said network;

a processor coupled to said first interface and said second interface; and

a device address retriever coupled to said processor for retrieving a first device address for said intelligent device from a network server of said network and for assigning a second device address to said electronic device.

121. An intelligent device as recited in Claim 120 wherein said first device address and said second device address are IP

addresses.

122. An intelligent device as recited in Claim 121 wherein said network server is a DHCP server.

123. An intelligent device as recited in Claim 121 wherein said first device address is the same as said second device address.

124. An intelligent device as recited in Claim 121 wherein said first device address is a global device address.

125. An intelligent device as recited in Claim 121 wherein said second device address is a private device address.

126. An intelligent device for performing device address assigning functionality, said intelligent device having a first device address, said intelligent device comprising:

a first interface for communicatively coupling said intelligent device to a network;

a second interface for communicatively coupling said intelligent device to a plurality of electronic devices such that each said electronic device is communicatively coupled to said network;

a processor coupled to said first interface and said second interface; and

a device address assignor coupled to said processor for assigning a second device address to said electronic device.

127. An intelligent device as recited in Claim 126 wherein said first device address and said second device address are IP addresses.

128. An intelligent device as recited in Claim 126 wherein said device address assignor is a DHCP server.

129. An intelligent device as recited in Claim 126 wherein said first device address is the same as said second device address.

130. An intelligent device as recited in Claim 126 wherein said first device address is a global device address.

131. An intelligent device as recited in Claim 126 wherein said second device address is a private device address.

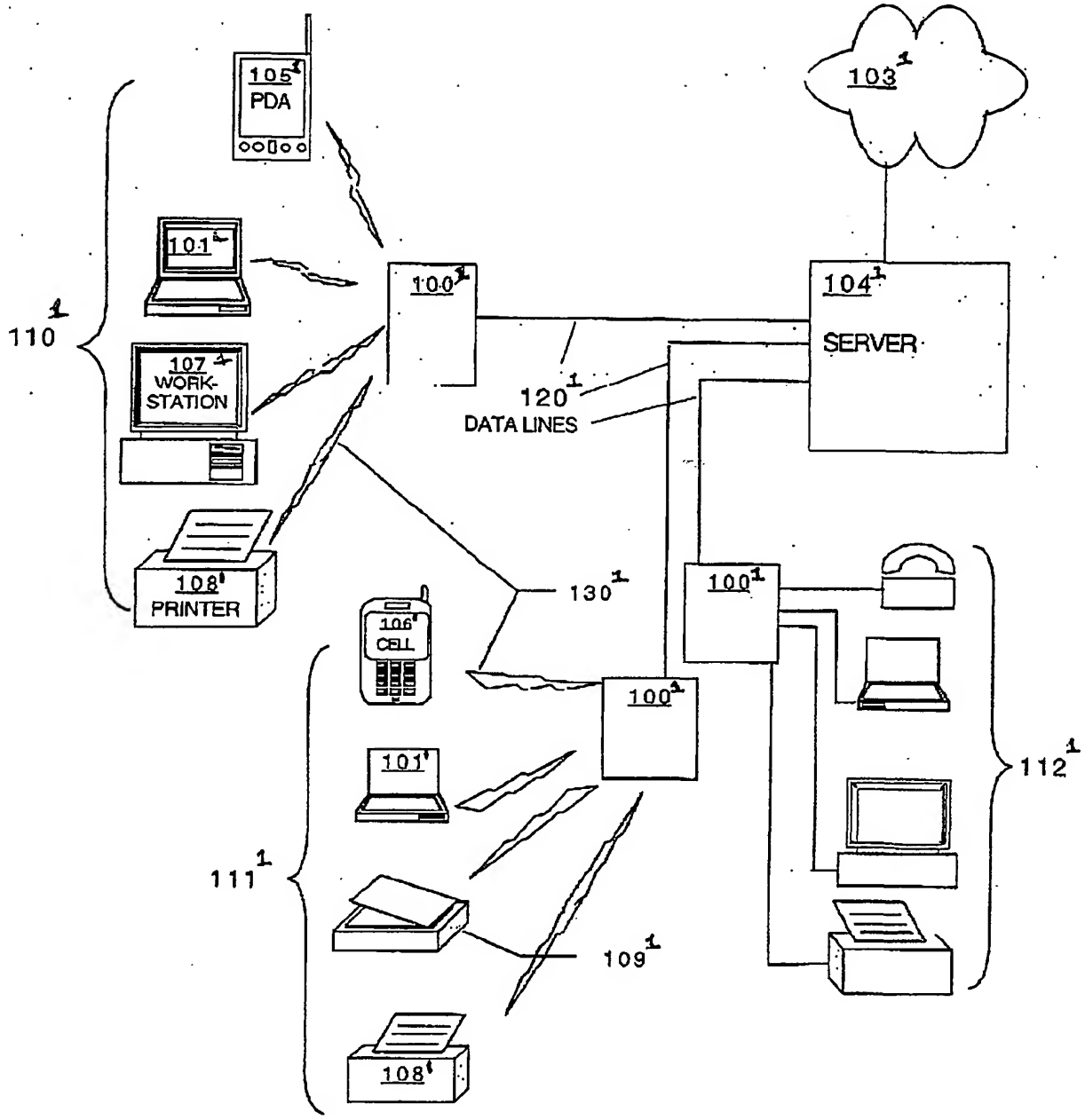

105
PDA
103
101
100
104
SERVER
110
107
WORK-
STATION
120
DATA LINES
108
PRINTER
130
100
106
CELL
100
101
112
111
109
108

FIGURE 1

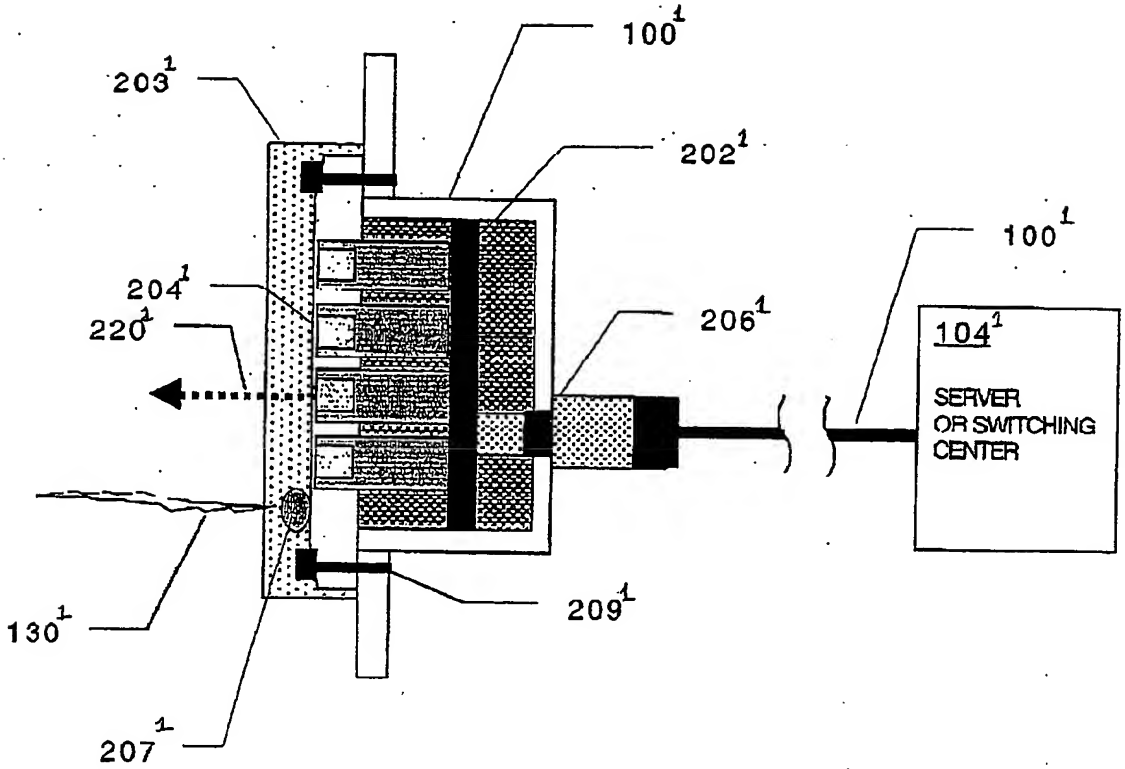

100 1
203 1
202 1
100 1
204 1
220 1
206 1
104 1
SERVER
OR SWITCHING
CENTER
130 1
209 1
207 1

FIGURE 2 1

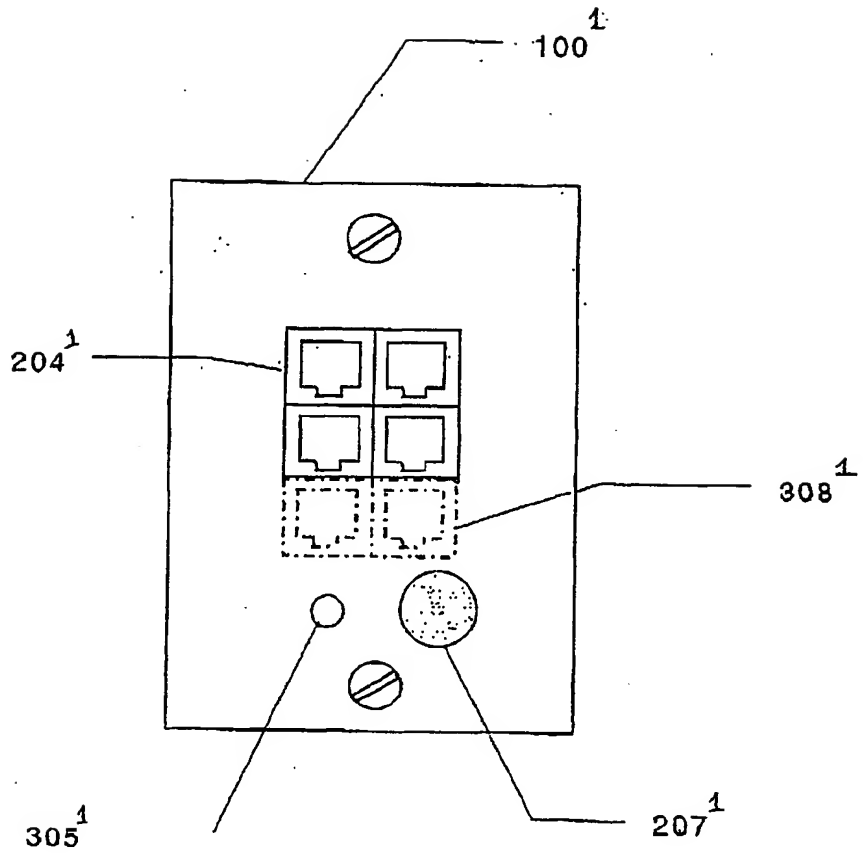


FIGURE 3 1

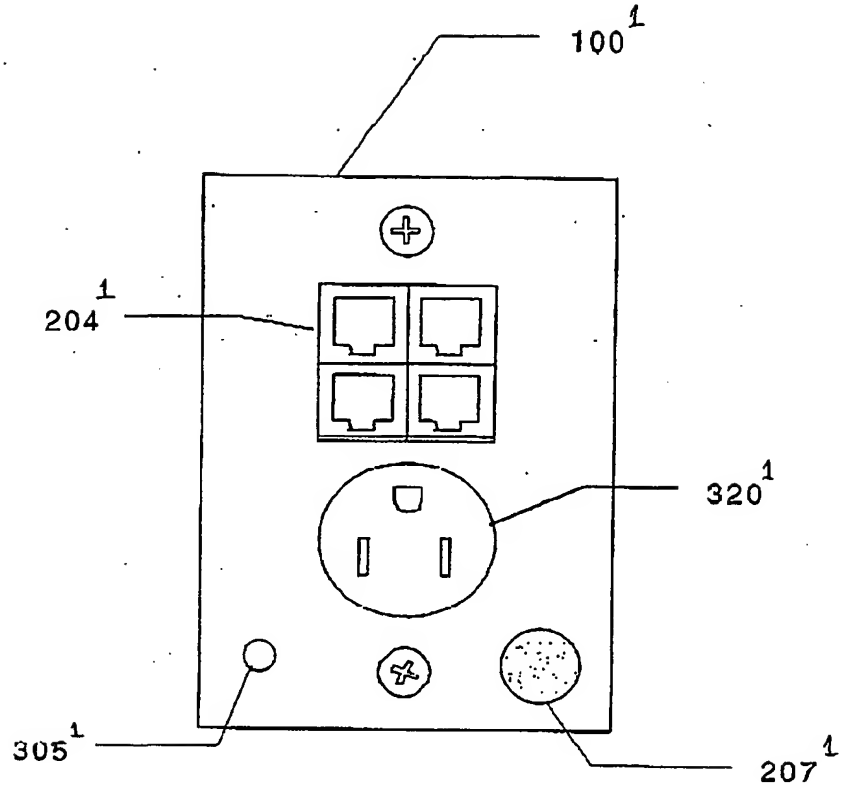


FIGURE 4 1

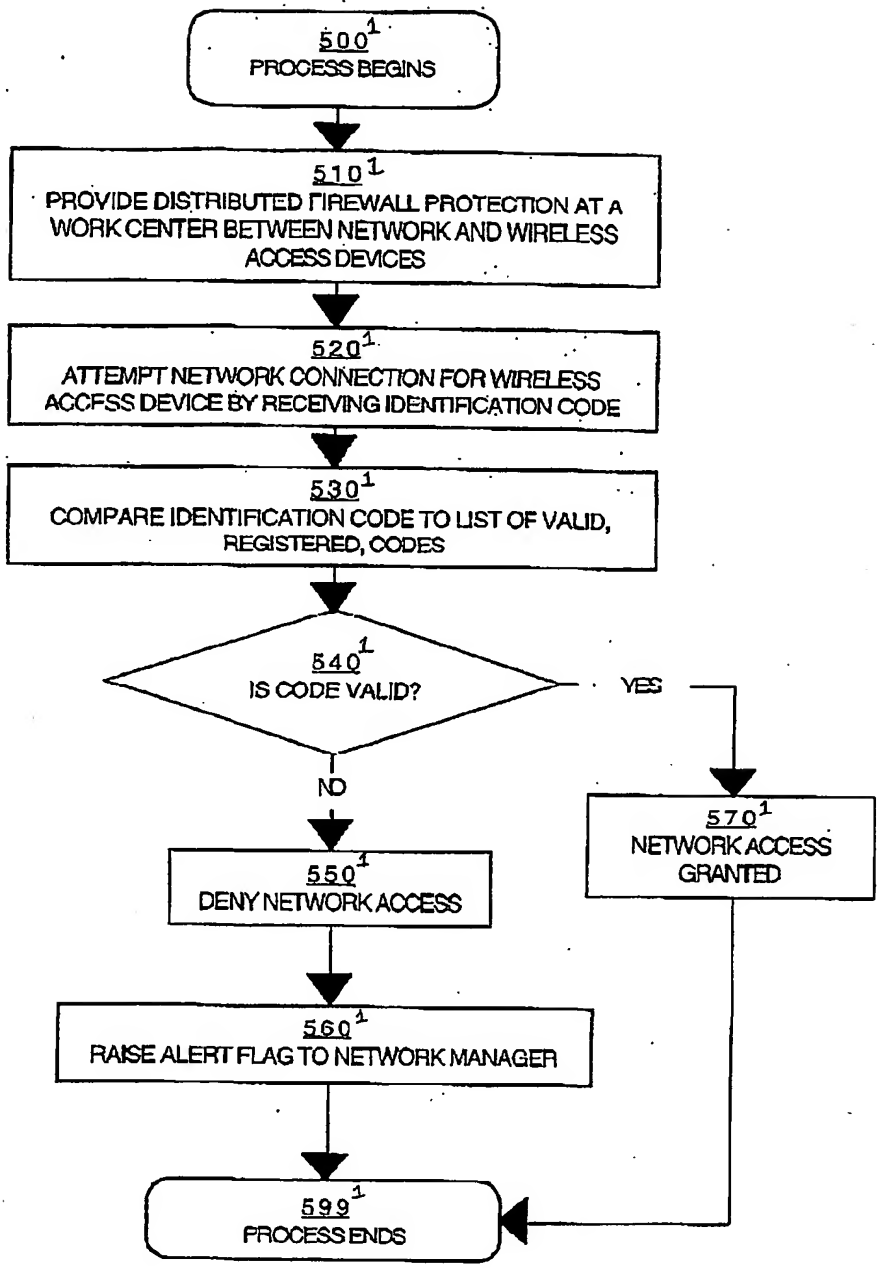

500 1
PROCESS BEGINS
510 1
PROVIDE DISTRIBUTED FIREWALL PROTECTION AT A WORK CENTER BETWEEN NETWORK AND WIRELESS ACCESS DEVICES
520 1
ATTEMPT NETWORK CONNECTION FOR WIRELESS ACCESS DEVICE BY RECEIVING IDENTIFICATION CODE
530 1
COMPARE IDENTIFICATION CODE TO LIST OF VALID, REGISTERED, CODES
540 1
IS CODE VALID?
YES
NO
570 1
NETWORK ACCESS GRANTED
550 1
DENY NETWORK ACCESS
560 1
RAISE ALERT FLAG TO NETWORK MANAGER
599 1
PROCESS ENDS

FIGURE 5 1

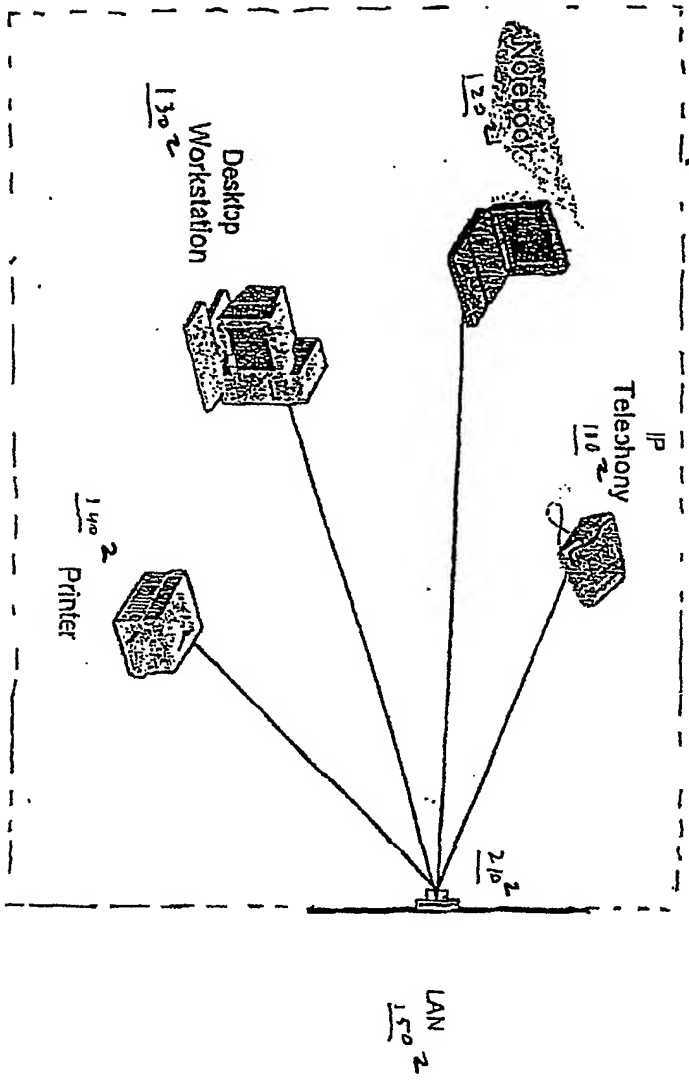

Notebook
120
Desktop
Workstation
130
IP
Telephony
110
Printer
140
100
210
LAN
150

Figure 1

Figure 2

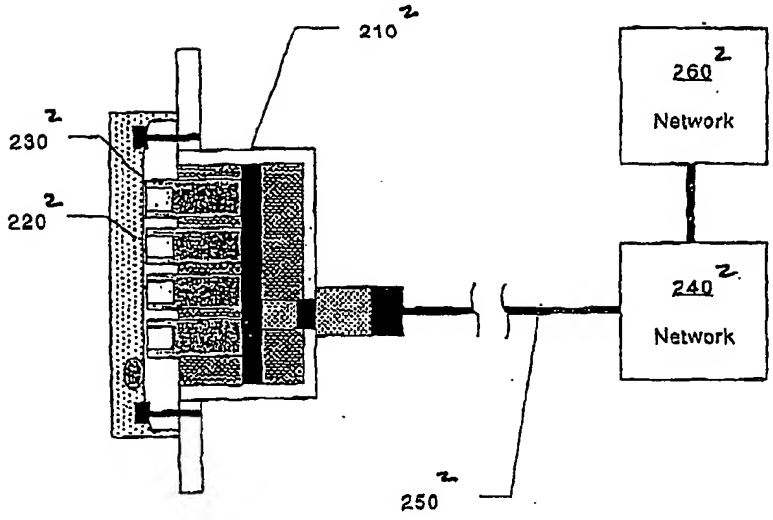


Figure 3

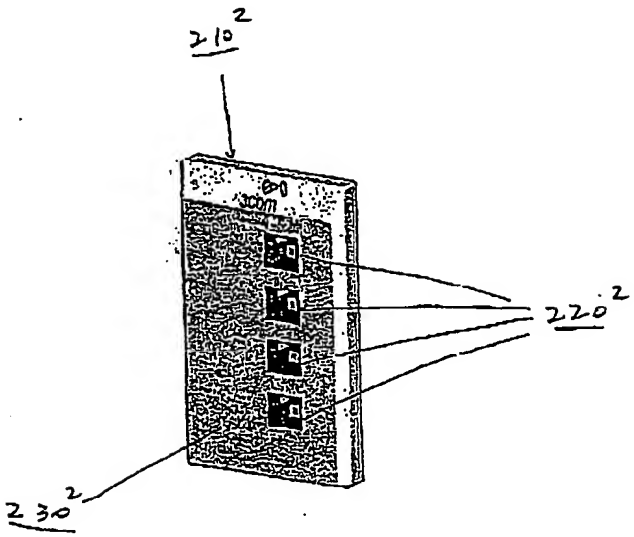


Figure 4

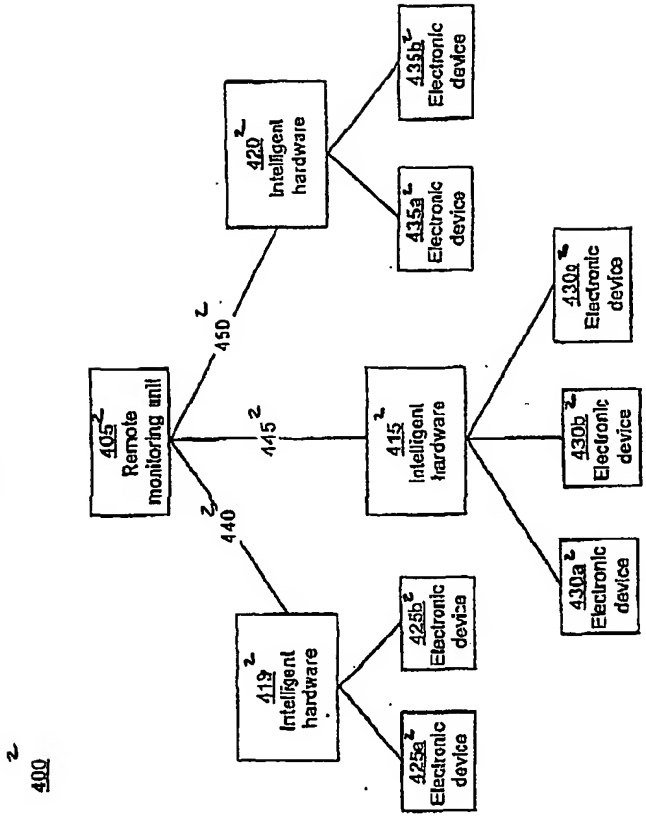

400
405 Remote monitoring unit
410 Intelligent hardware
415 Intelligent hardware
420 Intelligent hardware
425a Electronic device
425b Electronic device
430a Electronic device
430b Electronic device
430c Electronic device
435a Electronic device
435b Electronic device
440
445
450

Figure 5

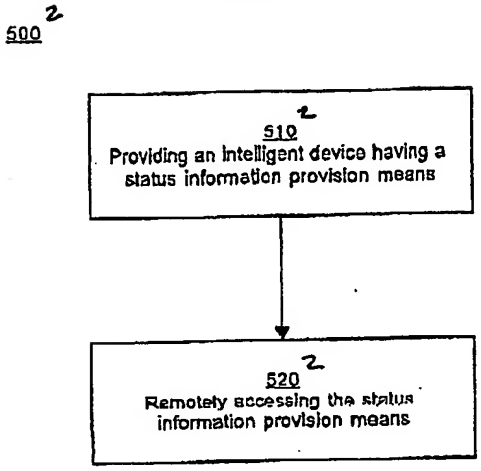
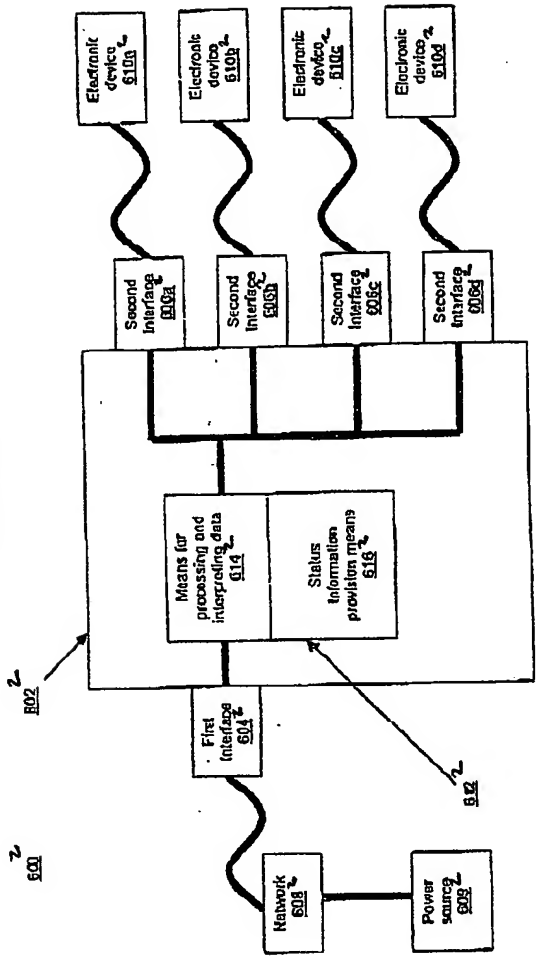

500
510
Providing an intelligent device having a status information provision means
520
Remotely accessing the status information provision means

Figure 6


Electronic device 610a
Electronic device 610b
Electronic device 610c
Electronic device 610d
Second interface 606a
Second interface 606b
Second interface 606c
Second interface 606d
Means for processing and interpreting data 614
Status information provision means 616
802
First interface 604
612
600
Network 608
Power source 609

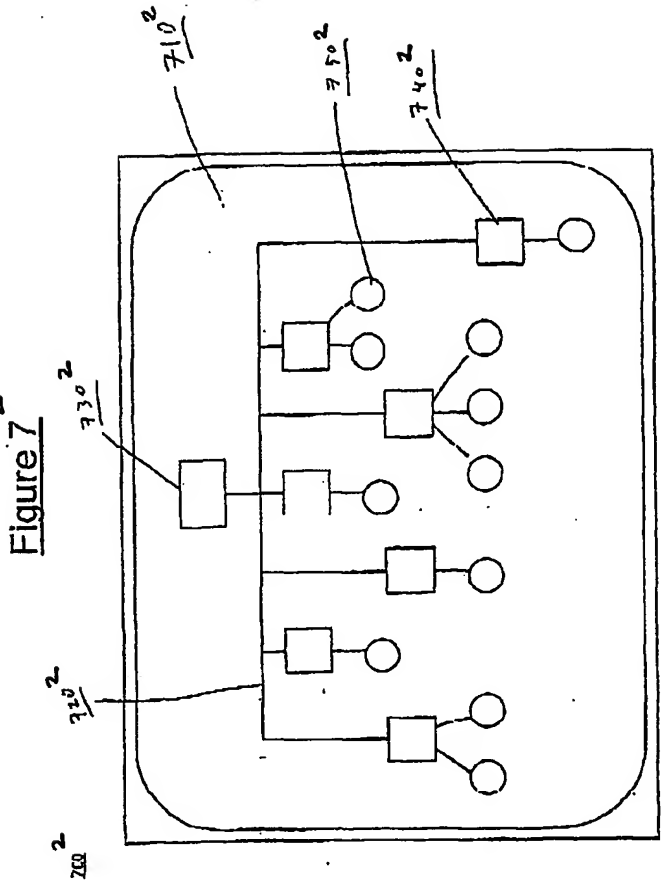
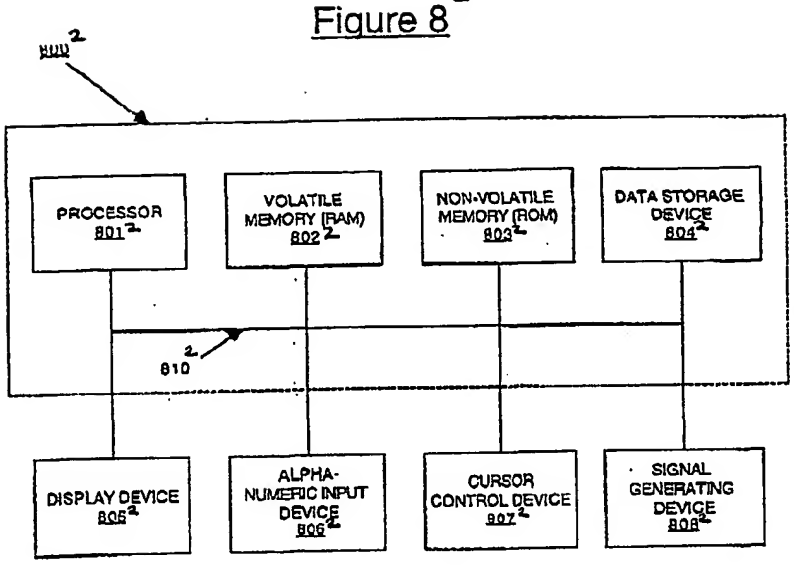


Figure 7

Figure 8


800
PROCESSOR
801
VOLATILE MEMORY (RAM)
802
NON-VOLATILE MEMORY (ROM)
803
DATA STORAGE DEVICE
804
810
DISPLAY DEVICE
805
ALPHA-NUMERIC INPUT DEVICE
806
CURSOR CONTROL DEVICE
807
SIGNAL GENERATING DEVICE
808

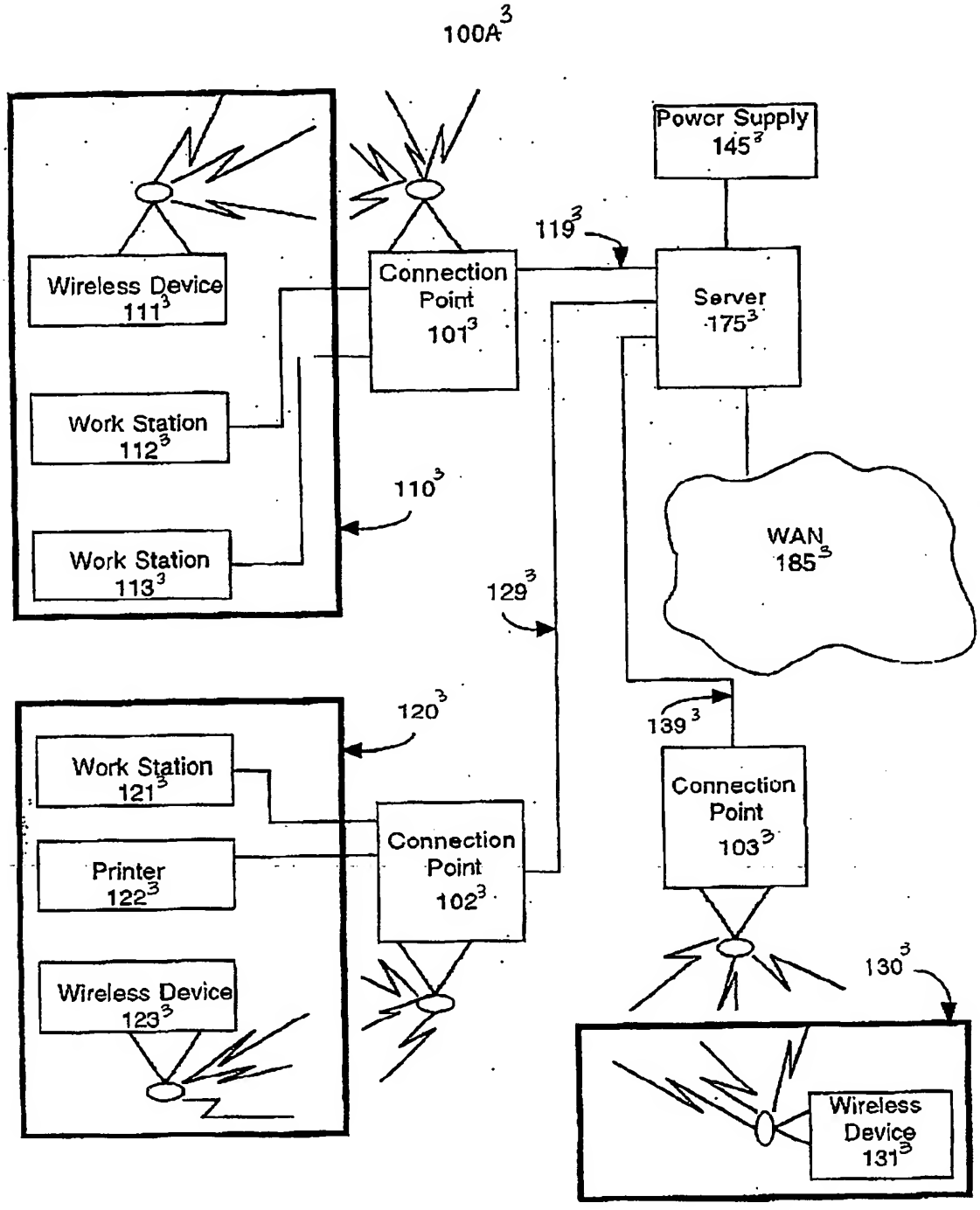

100A3
Power Supply
145 3
119 3
Wireless Device
111 3
Connection
Point
101 3
Server
175 3
Work Station
112 3
110 3
Work Station
113 3
WAN
185 3
129 3
120 3
139 3
Work Station
121 3
Connection
Point
103 3
Printer
122 3
Connection
Point
102 3
130 3
Wireless Device
123 3
Wireless
Device
131 3

Fig 1A3

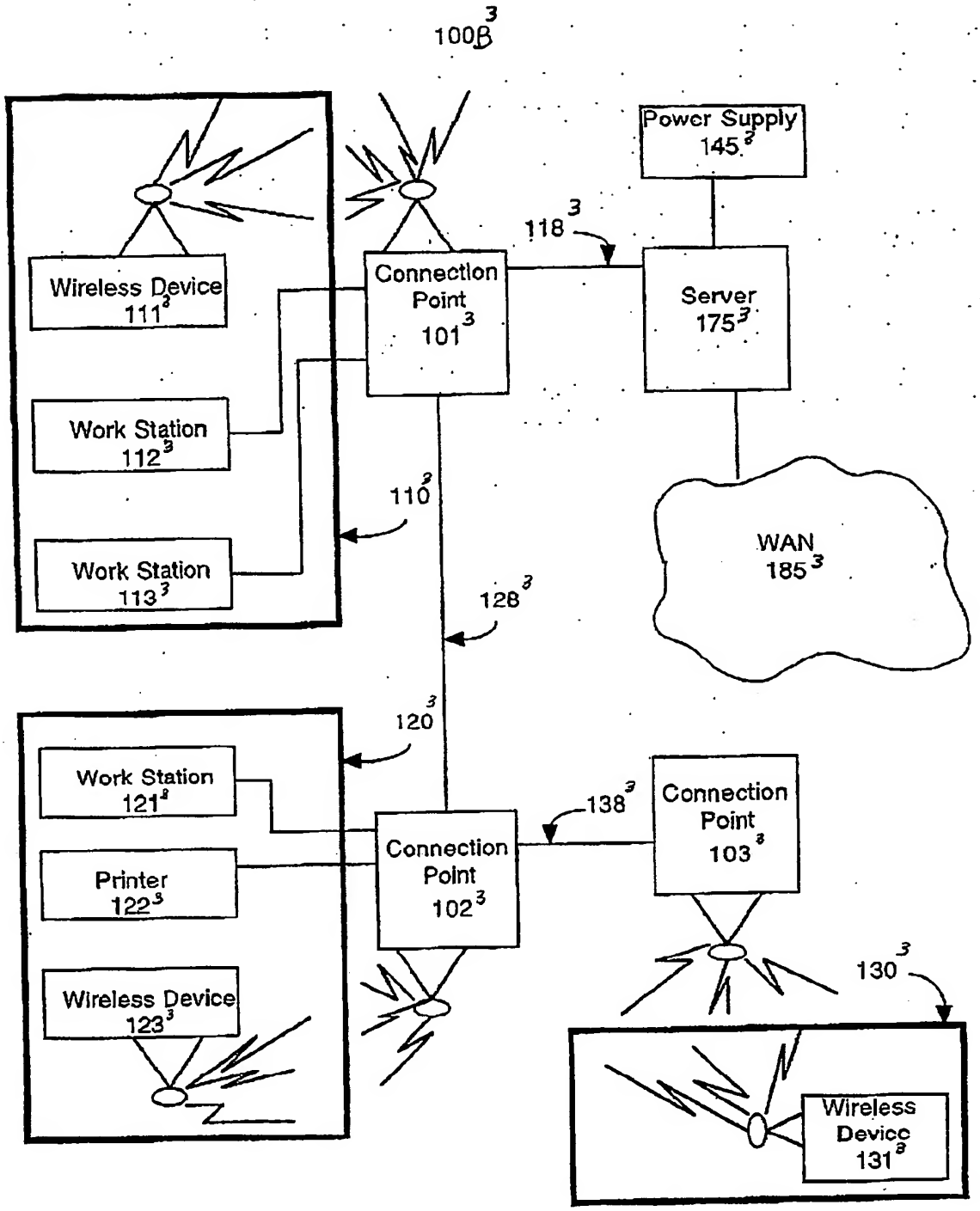

100B
Power Supply
145
118
Wireless Device
111
Connection
Point
101
Server
175
Work Station
112
110
WAN
185
Work Station
113
128
120
Work Station
121
Connection
Point
102
138
Connection
Point
103
Printer
122
130
Wireless Device
123
Wireless
Device
131

FIG 1 B

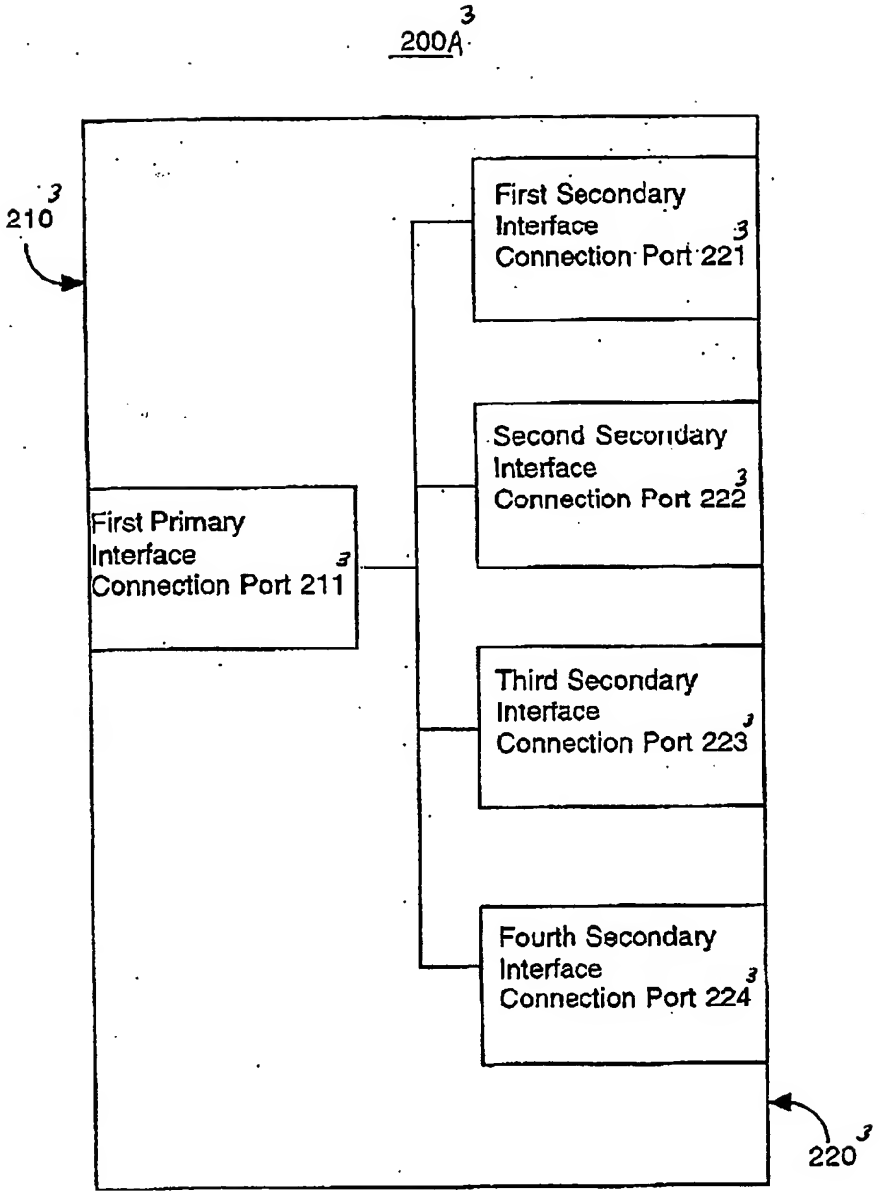

200A
210
First Secondary Interface Connection Port 221
Second Secondary Interface Connection Port 222
First Primary Interface Connection Port 211
Third Secondary Interface Connection Port 223
Fourth Secondary Interface Connection Port 224
220

FIG 2A

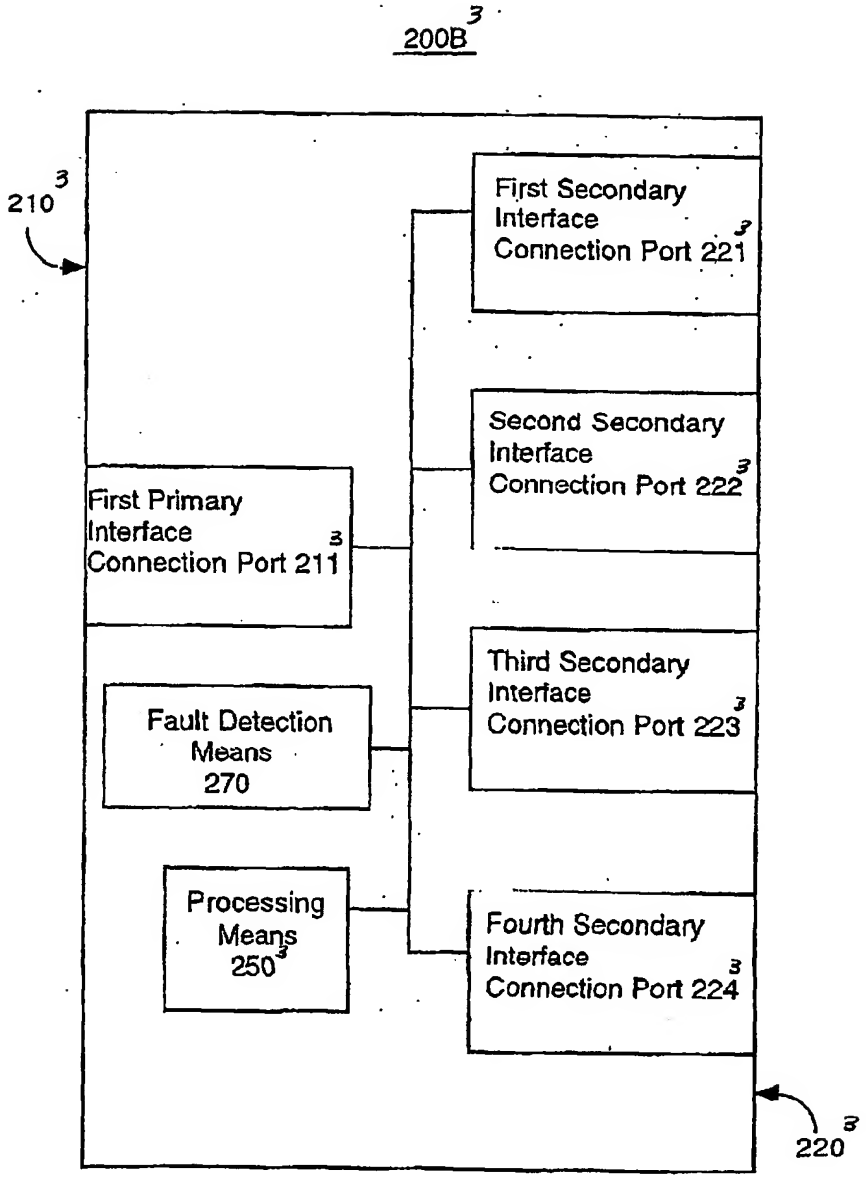

200B
210
First Secondary Interface Connection Port 221
Second Secondary Interface Connection Port 222
First Primary Interface Connection Port 211
Third Secondary Interface Connection Port 223
Fault Detection Means 270
Processing Means 250
Fourth Secondary Interface Connection Port 224
220

FIG 2B

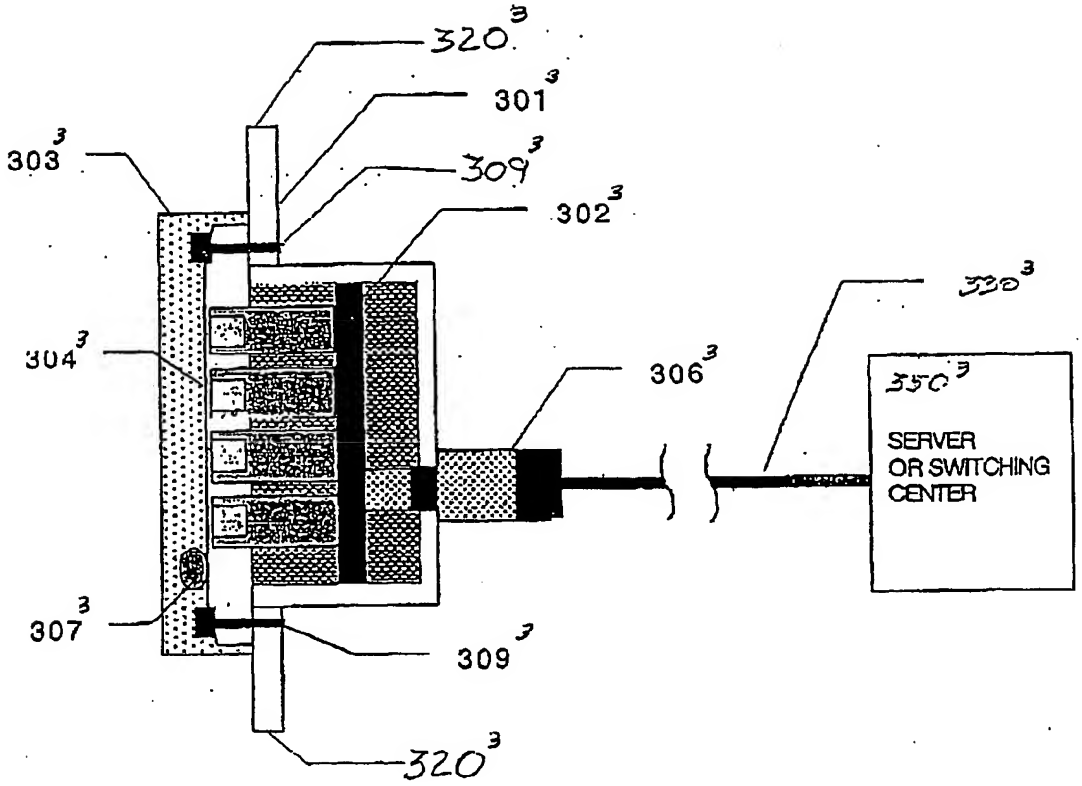

320
301
303
309
302
330
304
306
350
SERVER
OR SWITCHING
CENTER
307
309
320

FIGURE 3

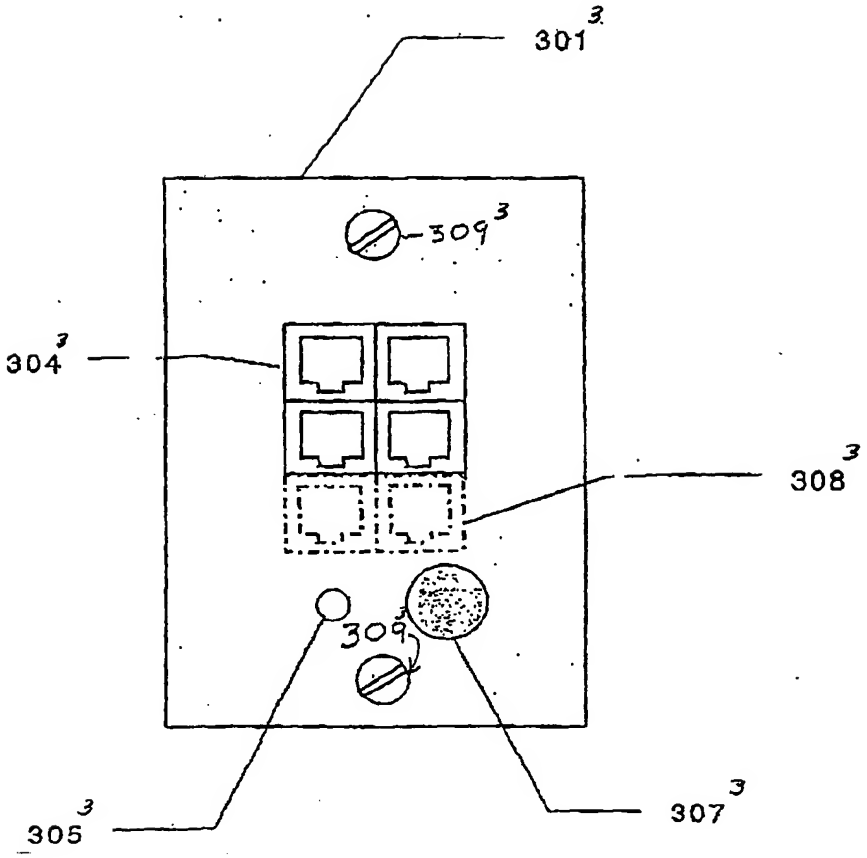


FIGURE 4

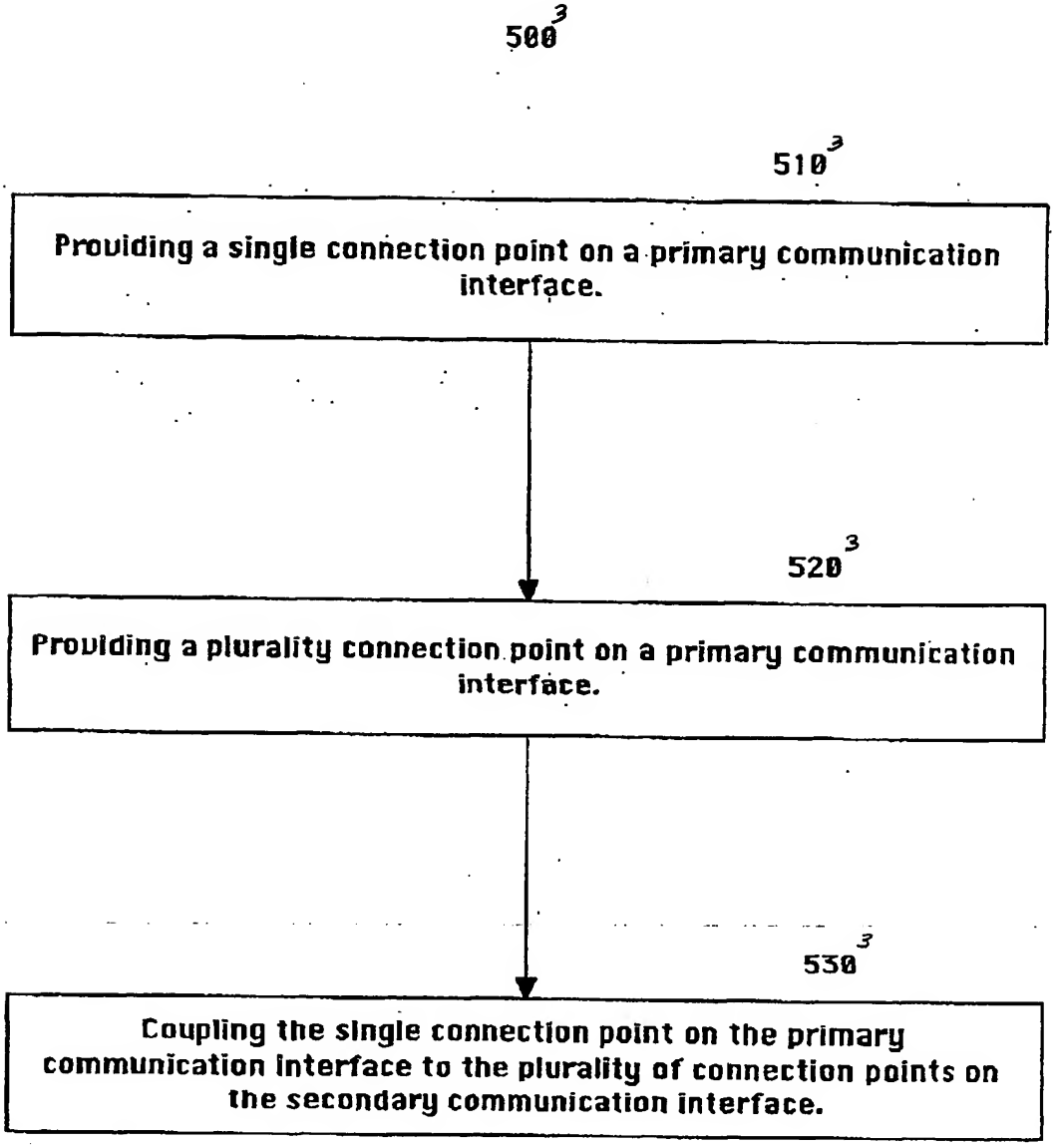

500
510
Providing a single connection point on a primary communication interface.
520
Providing a plurality connection point on a primary communication interface.
530
Coupling the single connection point on the primary communication interface to the plurality of connection points on the secondary communication interface.

FIG 5

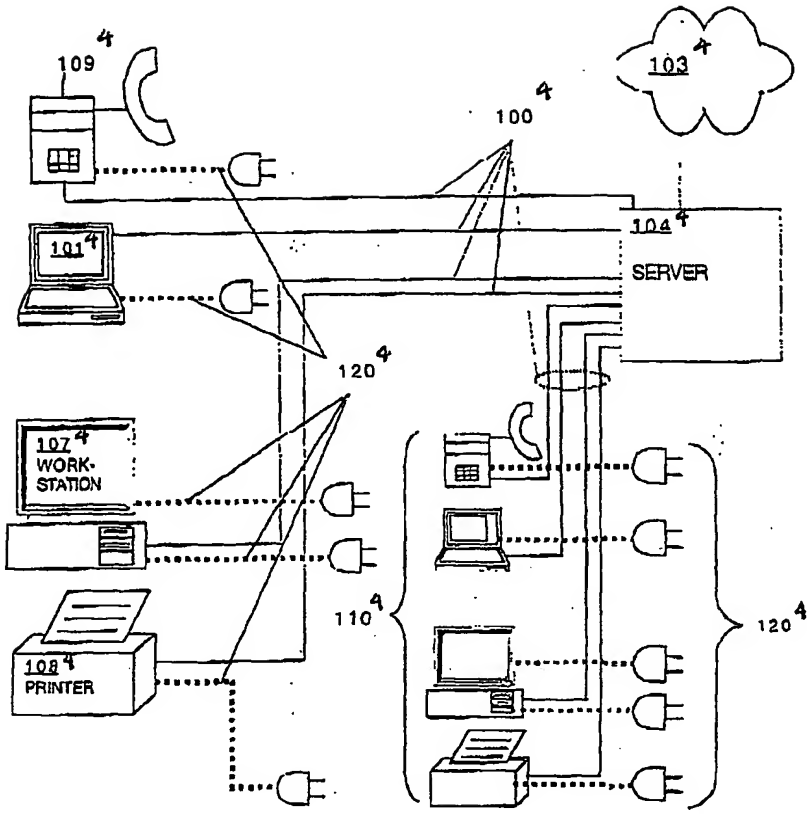


FIGURE 1
(PRIOR ART)

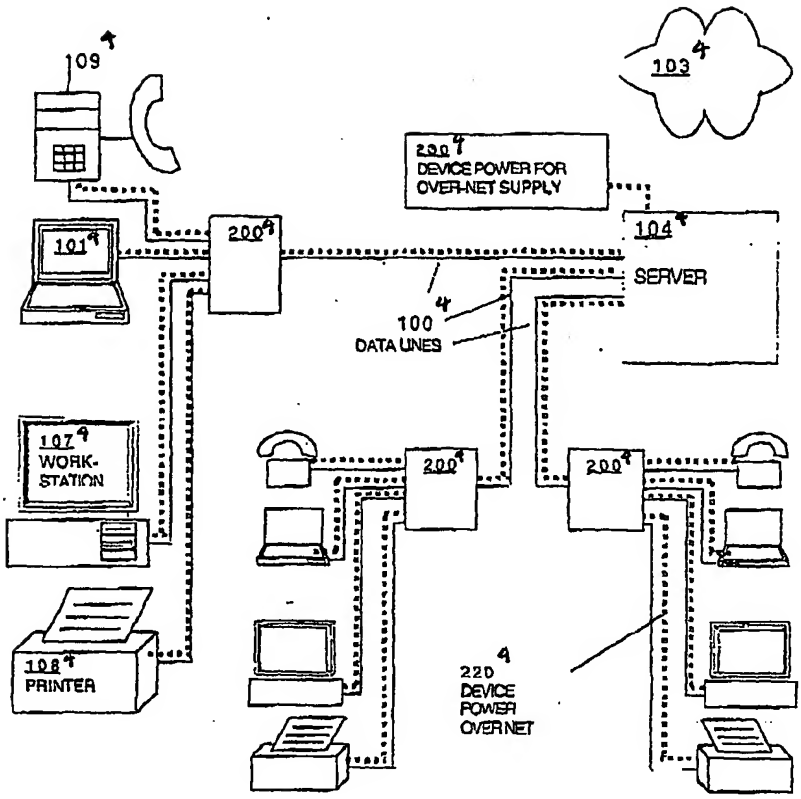

109
103
200
DEVICE POWER FOR OVER-NET SUPPLY
101
104
SERVER
100
DATA LINES
107
WORK-STATION
200
200
108
PRINTER
220
DEVICE POWER OVER NET

FIGURE 2A

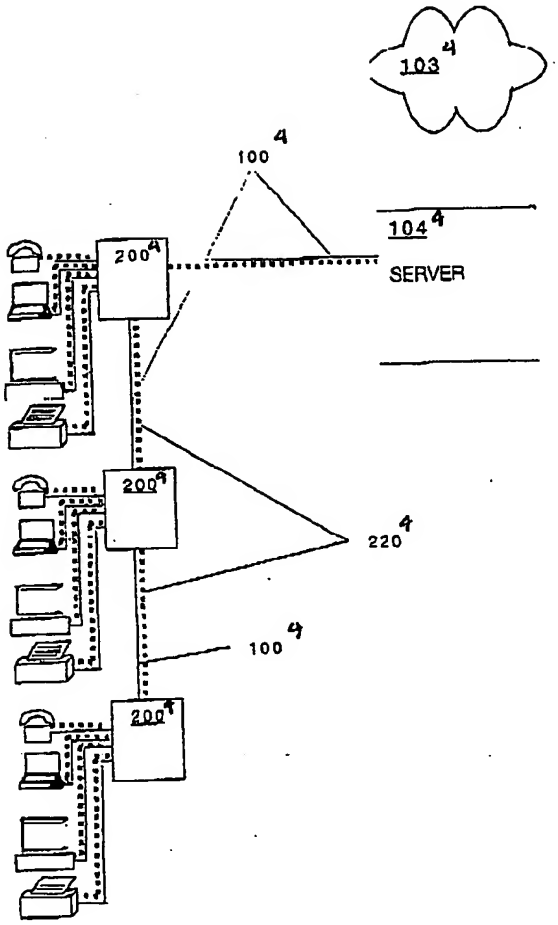


FIGURE 2B

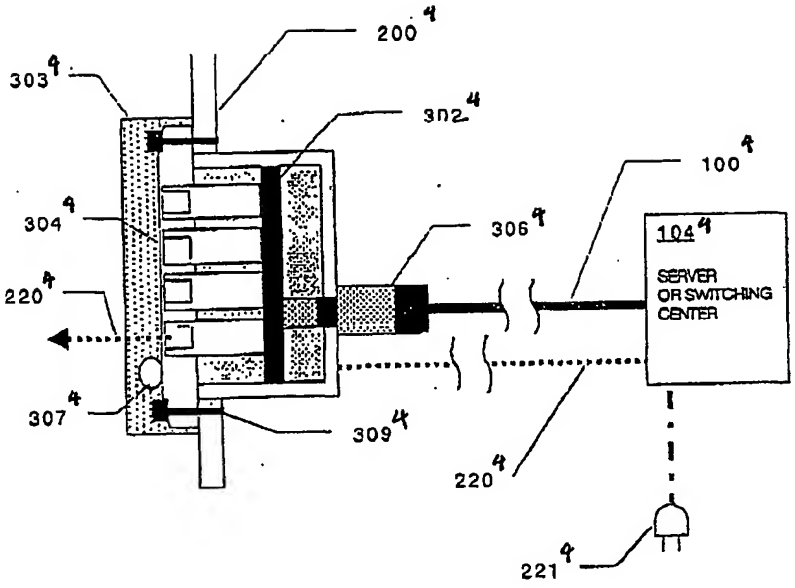

200
303
302
100
304
306
104
SERVER
OR SWITCHING
CENTER
220
307
309
220
221

FIGURE 3

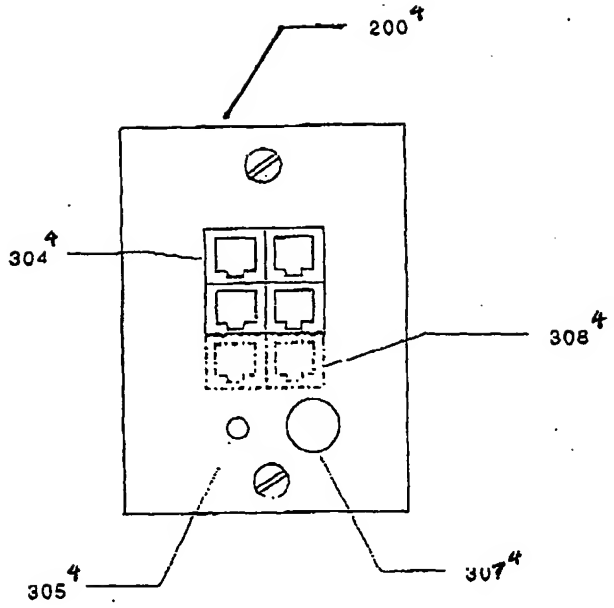


FIGURE 4A

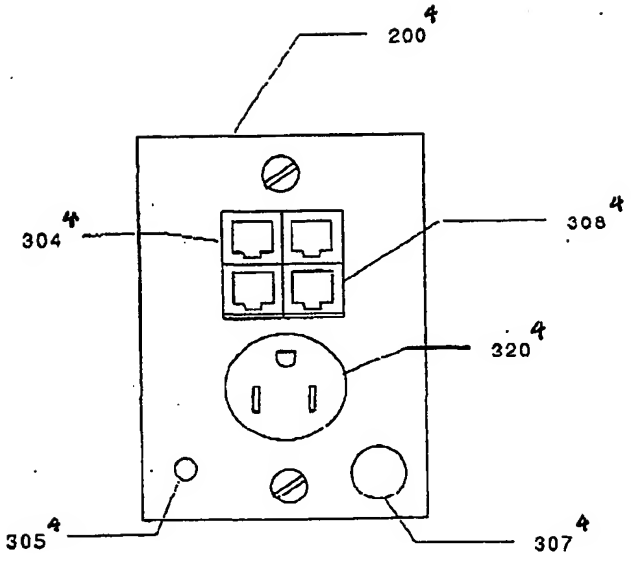


FIGURE 4B

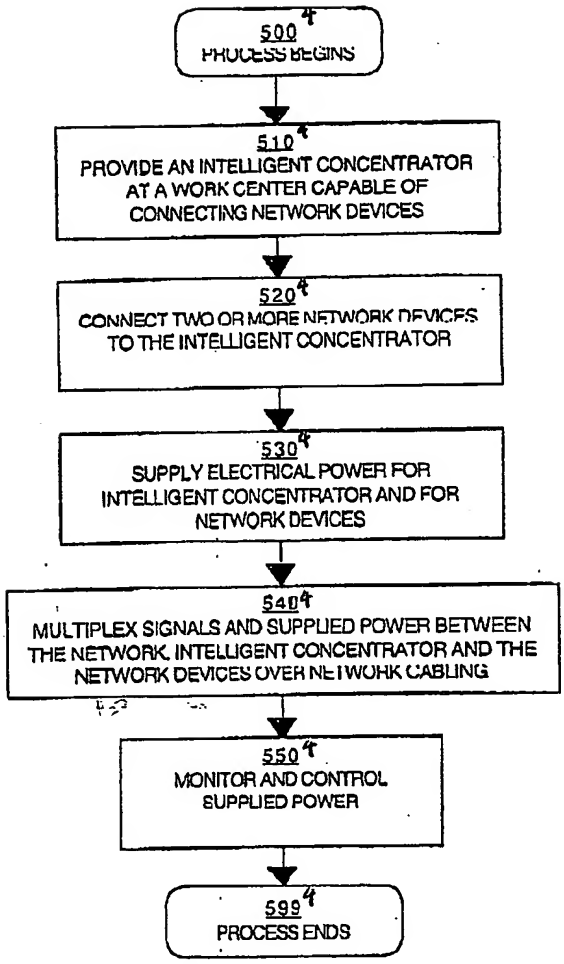

500
PROCESS BEGINS
510
PROVIDE AN INTELLIGENT CONCENTRATOR AT A WORK CENTER CAPABLE OF CONNECTING NETWORK DEVICES
520
CONNECT TWO OR MORE NETWORK DEVICES TO THE INTELLIGENT CONCENTRATOR
530
SUPPLY ELECTRICAL POWER FOR INTELLIGENT CONCENTRATOR AND FOR NETWORK DEVICES
540
MULTIPLEX SIGNALS AND SUPPLIED POWER BETWEEN THE NETWORK, INTELLIGENT CONCENTRATOR AND THE NETWORK DEVICES OVER NETWORK CABLING
550
MONITOR AND CONTROL SUPPLIED POWER
599
PROCESS ENDS

FIGURE 5

Figure 1

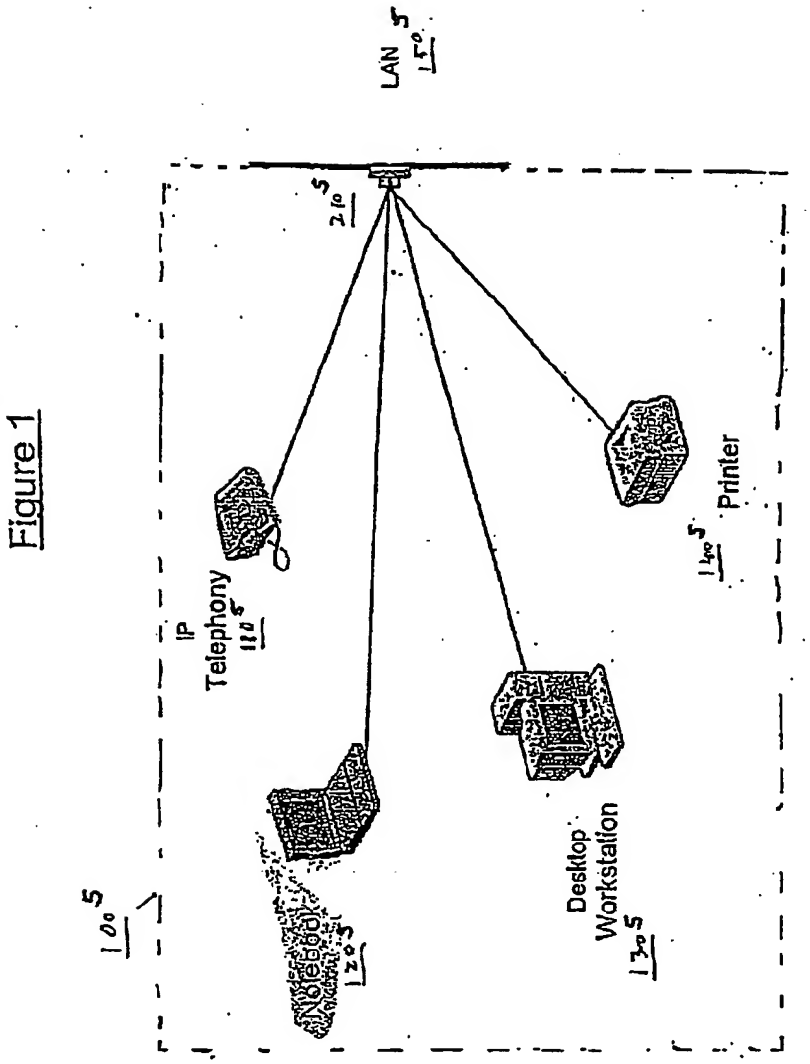


Figure 2

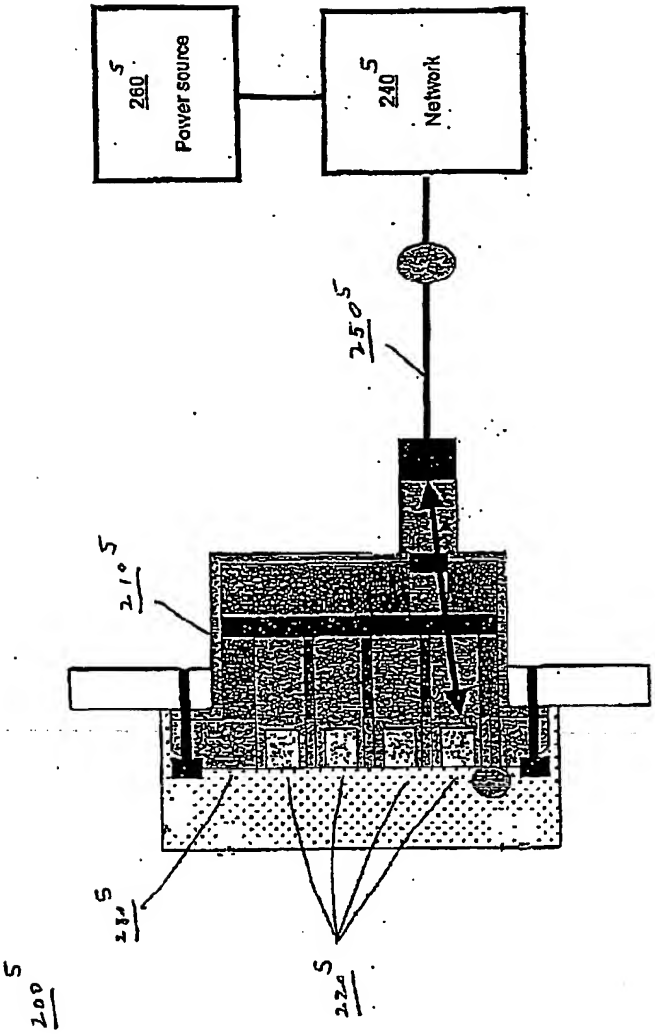


Figure 3

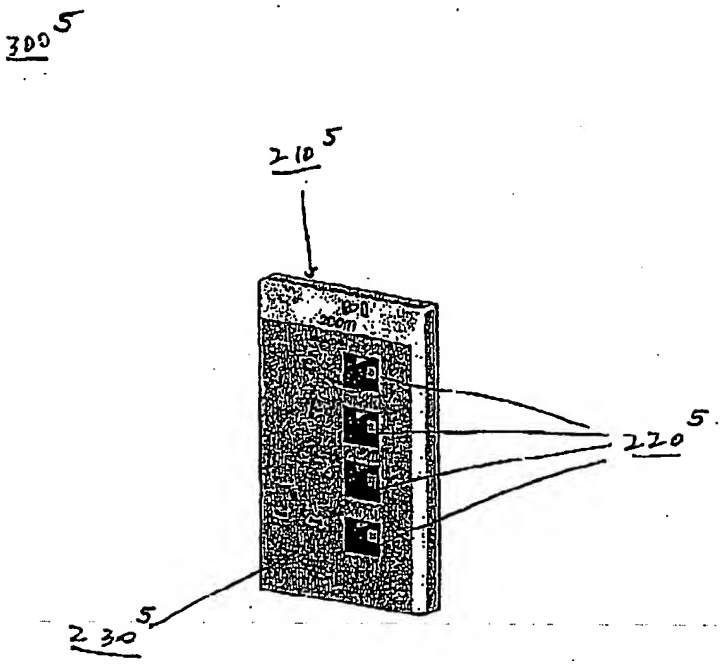


Figure 4

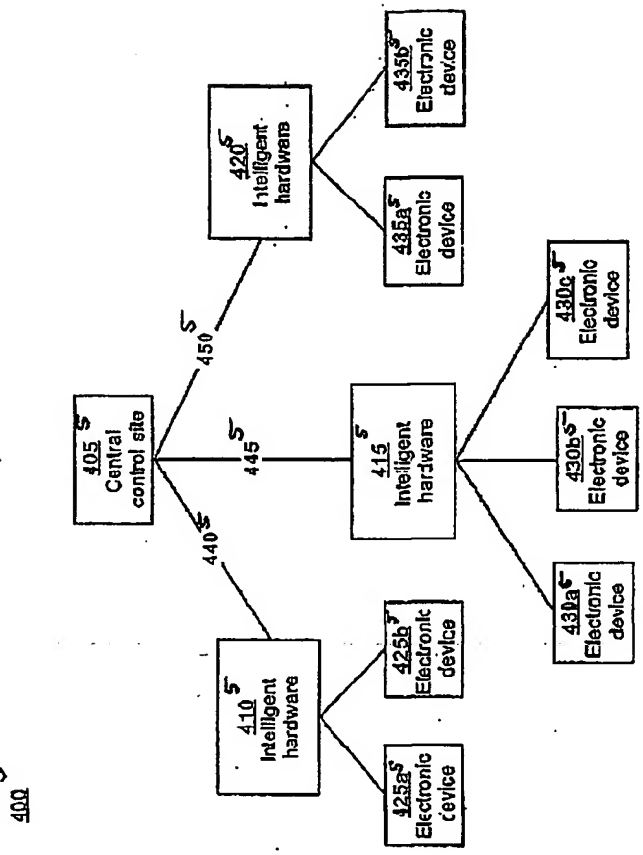

400
405 Central control site
410 Intelligent hardware
415 Intelligent hardware
420 Intelligent hardware
425a Electronic device
425b Electronic device
430a Electronic device
430b Electronic device
430c Electronic device
435a Electronic device
435b Electronic device
440
445
450

Figure 5

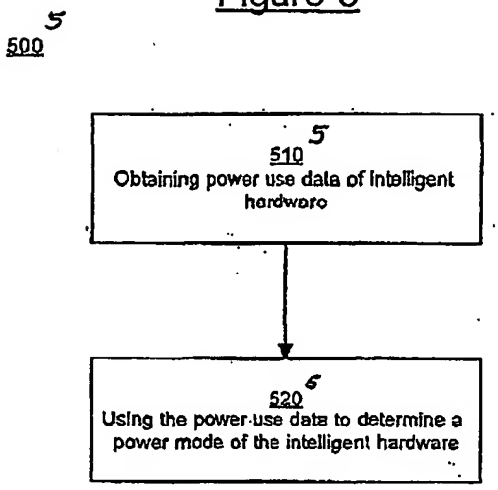

500
510
Obtaining power use data of intelligent hardware
520
Using the power use data to determine a power mode of the intelligent hardware

Figure 6

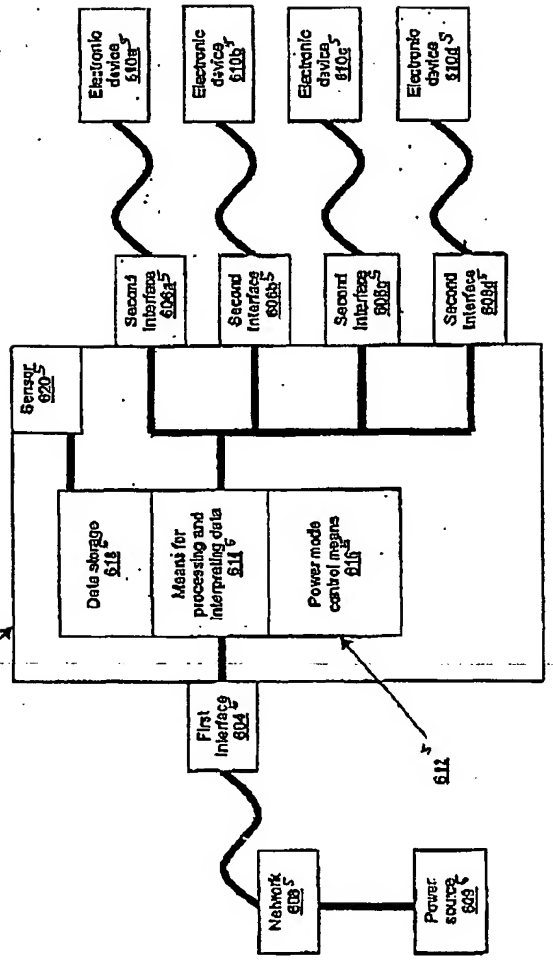

Electronic device 610a
Electronic device 610b
Electronic device 610c
Electronic device 610d
Second interface 608a
Second interface 608b
Second interface 608c
Second interface 608d
Sensor 620
Data storage 618
Means for processing and interpreting data 614
Power mode control means 616
First interface 604
Network 606
Power source 609
602
600
612

Figure 1

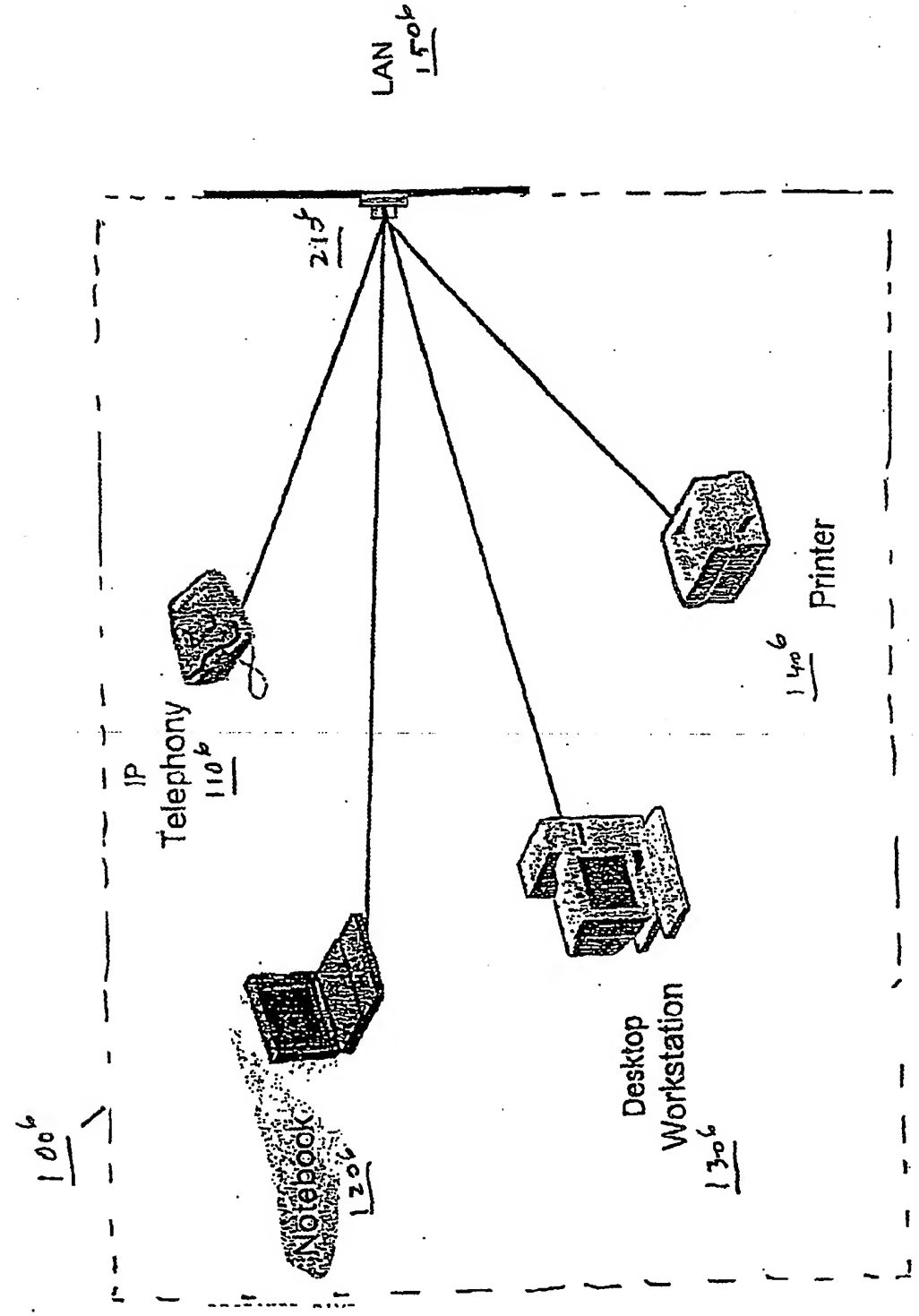

LAN
150
215
IP
Telephony
110
Printer
140
Desktop
Workstation
130
Notebook
120
100

Figure 2

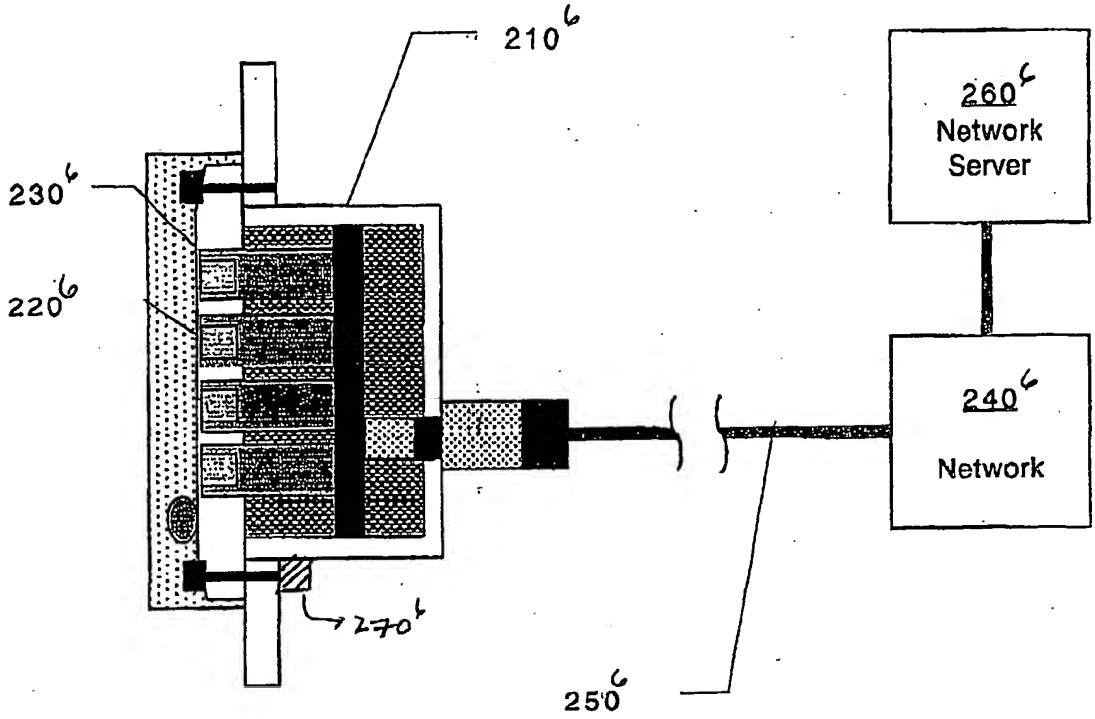


Figure 3b

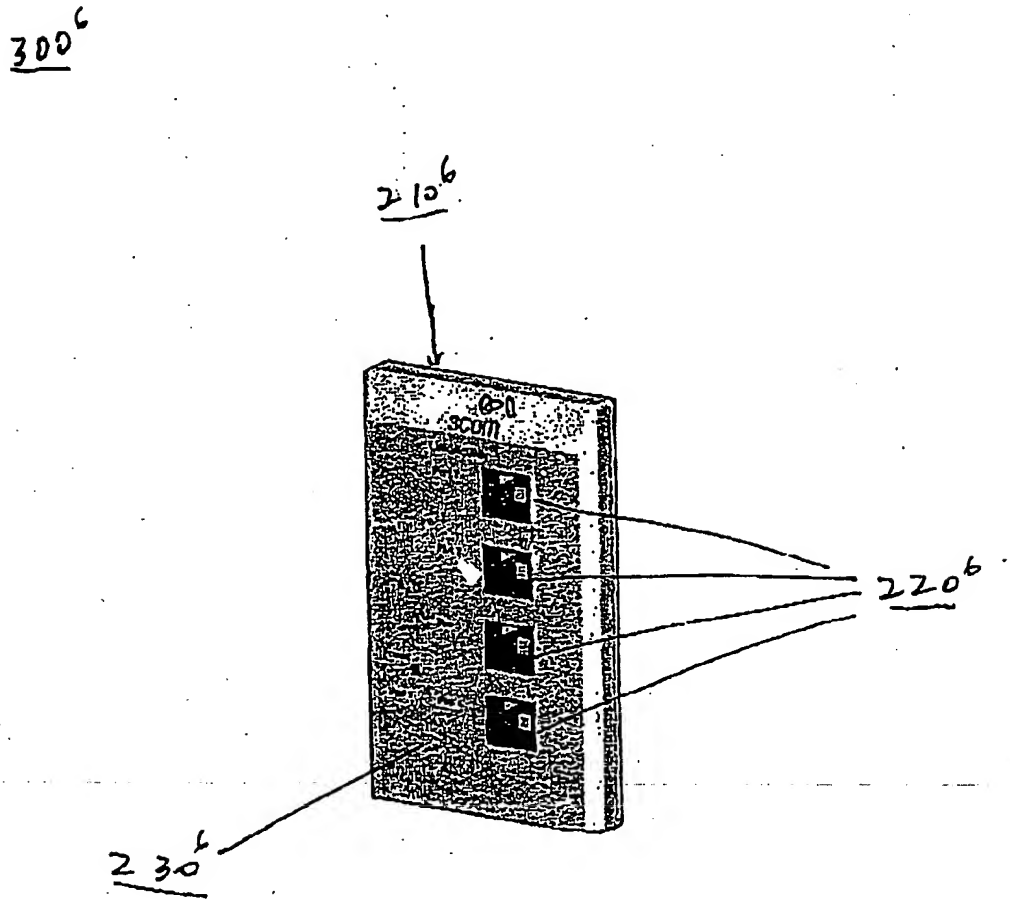


Figure 4

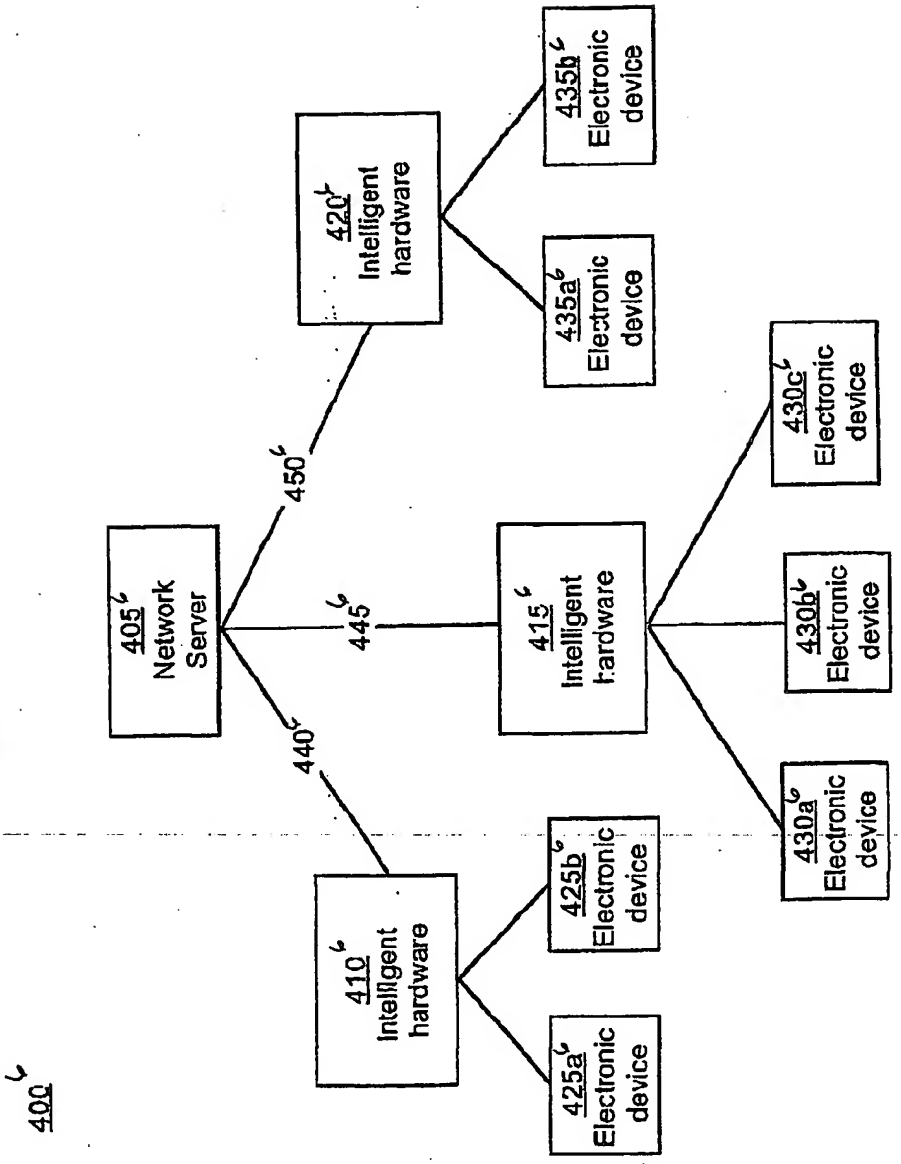

400
405 Network Server
410 Intelligent hardware
415 Intelligent hardware
420 Intelligent hardware
425a Electronic device
425b Electronic device
430a Electronic device
430b Electronic device
430c Electronic device
435a Electronic device
435b Electronic device
440
445
450

Figure 5

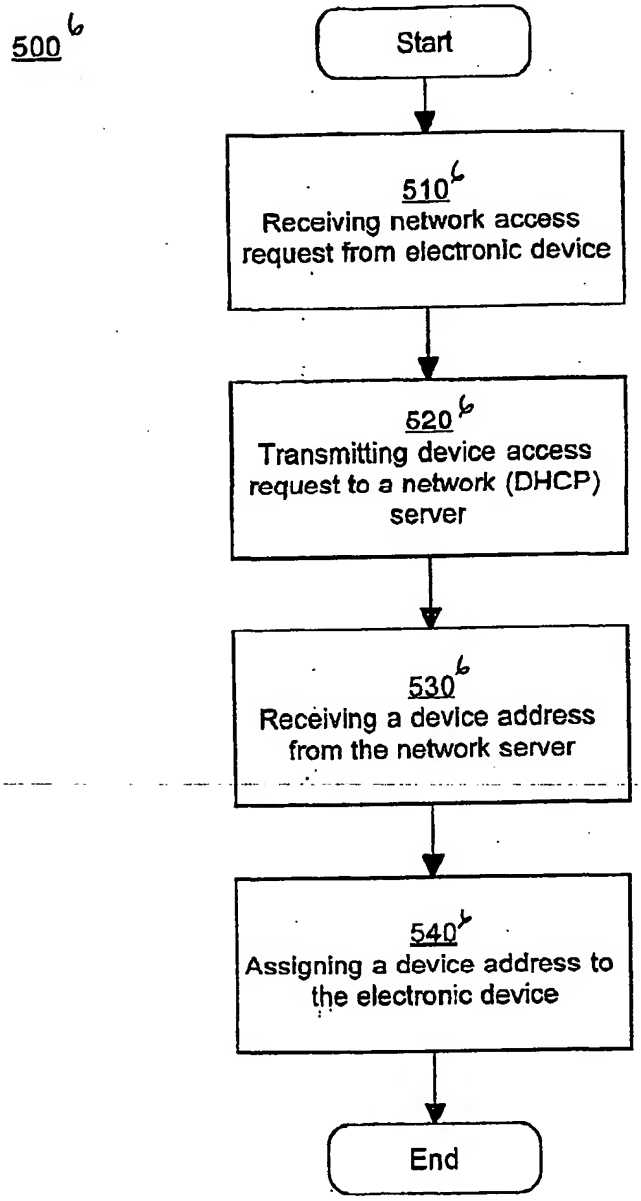

500
Start
510
Receiving network access request from electronic device
520
Transmitting device access request to a network (DHCP) server
530
Receiving a device address from the network server
540
Assigning a device address to the electronic device
End

Figure 6

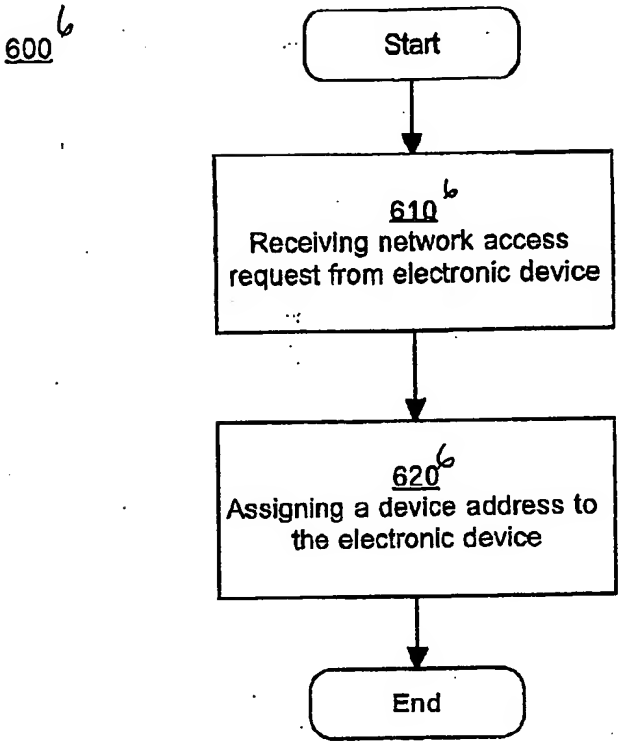

600
Start
610
Receiving network access request from electronic device
620
Assigning a device address to the electronic device
End

Figure 7

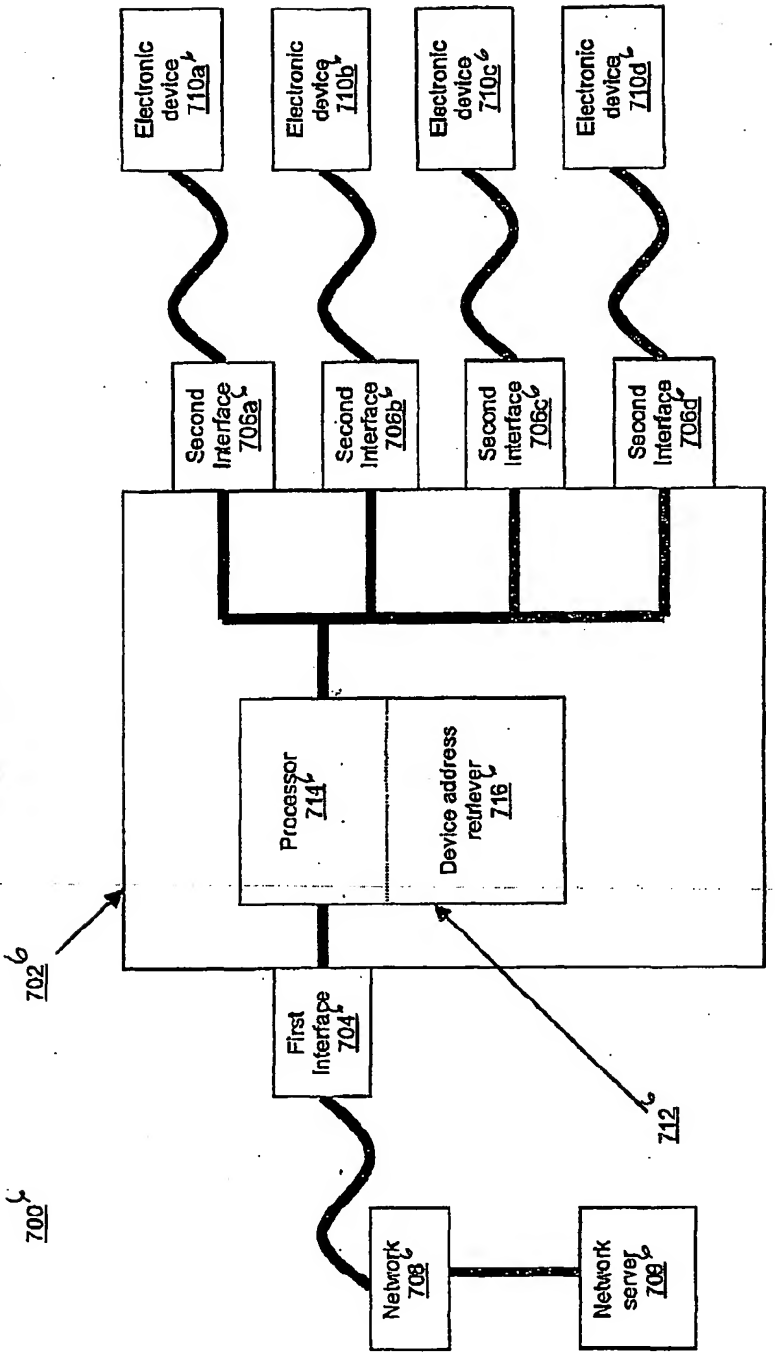
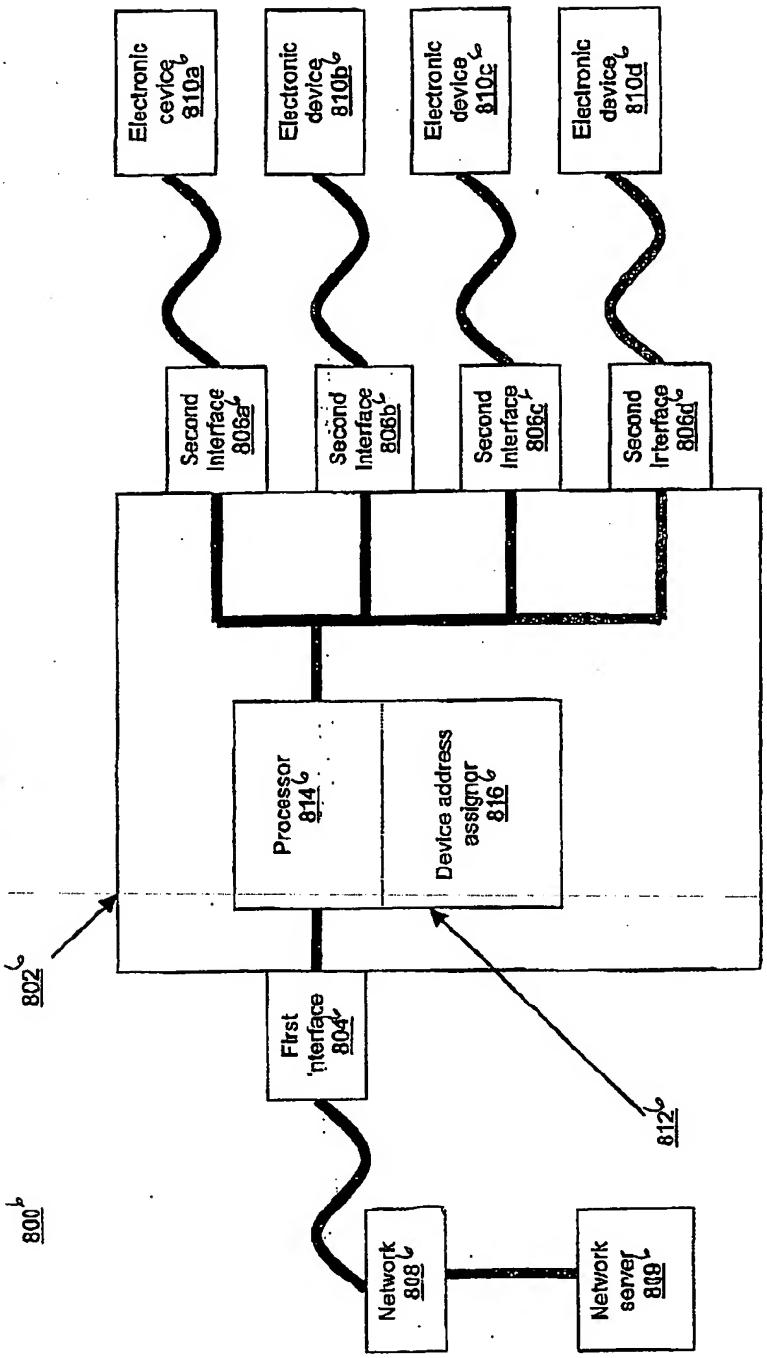

Electronic device 710a
Electronic device 710b
Electronic device 710c
Electronic device 710d
Second Interface 706a
Second Interface 706b
Second Interface 706c
Second Interface 706d
Processor 714
Device address retriever 716
702
First Interface 704
712
700
Network 708
Network server 709

Figure 8


Electronic device 810a
Electronic device 810b
Electronic device 810c
Electronic device 810d
Second Interface 806a
Second Interface 806b
Second Interface 806c
Second Interface 806d
Processor 814
Device address assignor 816
802
First Interface 804
812
800
Network 808
Network server 809